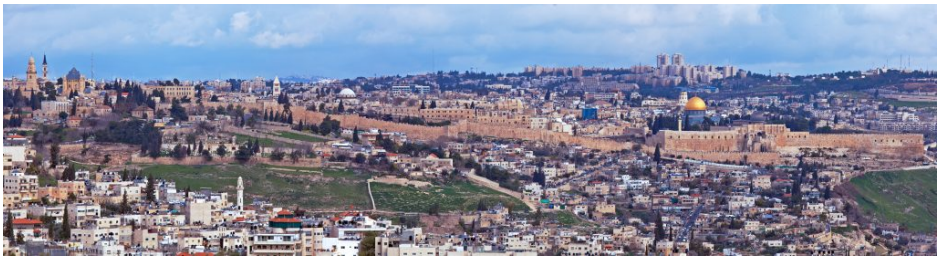
JCT
LEV ACADEMIC CENTER

ACA 2017

23rd Conference on Applications of Computer Algebra

Jerusalem, July 17–21, 2017

Commemorating the heritage of Jonathan Michael Borwein



Book of Abstracts

Thierry Dana-Picard and Ilias Kotsireas
with Aharon Naiman

Contents

Invited Speakers

Session chairs:

Ilias Kotsireas
Wilfrid Laurier University, ON, Canada

Thierry Dana-Picard
Jerusalem College of Technology, Israel

Teaching Math to Lady M

Bruno Buchberger

Bruno Buchberger Research Institute for Symbolic Computation Johannes Kepler University, Linz / Hagenberg Castle, Austria

I stopped teaching logic and math to humans. Instead I started to teach logic / math to Lady M, a machine. She (or he or it) has absolutely no insight and I enjoy that she does not expect that what I am telling her has any meaning (semantics). For certain input expressions she produces certain output. Very reliably, for the same input the same output. By certain input, her inner state changes and she her input / output behavior changes. Recently, after many layers of communication, I managed to make her behave the way I behaved when, as a PhD student, I invented the Gröbner bases algorithm. I.e. I taught her to invent mathematical algorithms and proofs. Of course, she does not know. Of course, I cannot give a talk on this, since I stopped talking to mathematicians. However, if you like and you don't make me jealous, you may come and watch me talk to Lady M.

Gamma and Factorial in the Monthly

Rob Corless

Western University, London, ON, Canada

Since its inception in the 19th century, the American Mathematical Monthly has published over fifty papers on the Gamma function or equivalently the factorial function. Over half of these were on Stirling's formula. We survey these papers, which include a Chauvenet prize winning paper by Philip J. Davis [1] and a paper by the Fields medallist Manjul Bhargava [2], and highlight some features in common. We also identify some surprising gaps and attempt to fill them, especially on the "inverse Gamma function".

This is joint work with the late Jonathan M. Borwein.

References

[1] P. J. Davis. *Leonhard Euler's integral: A historical profile of the Gamma function: In memoriam: Milton Abramowitz* 66(10), 849-869 (1959).

[2] M. Bhargava. *The factorial function and generalizations*, American Mathematical Monthly 107 (9),pp. 783-799 (2000).

Enhancing Teachers' and Students' Mathematical Knowledge in a Technology-Rich Environment

Sara Hershkovitz

The Center for Educational Technology (CET) - Tel Aviv, Israel

In the last century, the main goals of mathematics education were based on conceptual understanding, problem solving and problem posing, modeling, application, reasoning, creativity, and critical thinking ([5], [3], [2]). These goals became possible with the development of technological tools (which had previously not existed) that could carry out the procedures. The integration of digital technology into the mathematics classroom is an ongoing process ([4]) which has also created an ability to focus teaching and learning processes on important ideas in mathematics. Today, with the aid of the new technologies, it is possible to develop learning approaches that include the use of representations, research into mathematical phenomena through dynamic technological applications, and feedback from the computer through mirroring ([6]) of the outcome of the student's action ("intellectual mirroring").

The feedback allows the student to solve problems, to research and test different alternatives and decide whether he has achieved what he set out to do, and, by testing , to generalize ideas and phenomena. Feedback is changed from a confirmation of prior knowledge - feed *back* - to the new knowledge - feed *forward*[1].

In addition, on the one hand, the technology facilitates the assembly of rich content to develop the required concepts and ideas, together with the disciplinary goals and learning skills. On the other hand it allows the students' learning abilities to be checked and analyzed using analytical tools applied to big data, collected and analyzed on an ongoing basis. Based on these data, teaching and learning processes appropriate to each student can be constructed ([7]). These new possibilities carry with them new ways of content development for all educational stages, and new methods for teacher development.

In the presentation, mathematics instruction will be presented and discussed as interaction of teachers, students, and content in technological learning environments ([1]).

[1] http://www.jisc.ac.uk/guides/feedback-and-feed-forward

References

[1] D.K. Cohen, S.W. Raudenbush and D.L. Ball. *Resources, instruction, and research*. Educational Evaluation and Policy Analysis, 25(2), 119-142 (2003).

[2] Common Core State Standards Initiative. Mathematics curriculum standards: http://www.corestandards.org/Math (2010)

[3] J. Kilpatrick, J. Swafford and B. Findell. *Adding It Up: Helping children learn mathematics*, Washington, DC: National Academy Press (2001).

[4] C. Laborde, and R. Straber. *Place and use of new technology in the teaching of mathematics: ICMI activities in the past 25 years*. ZDM, Int J Math Educ, 42(7), 121-133 (2010).

[5] NCTM - National Council of Teachers of Mathematics. Professional standards for teaching mathematics. Reston, VA (1991).

[6] Schwartz J. (1989). *Intellectual Mirrors: A Step in the Direction of Making Schools Knowledge-Making Places*, Harvard Educ Rev, 59 (1) 51-62.

[7] S. Steenbergen-Hu and H. Cooper. *A meta-analysis of the effectiveness of Intelligent Tutoring Systems on K-12 students' mathematical learning*, Journal of Educational Psychology, 105(4), 970-987 (2013).

Parallel Coordinates: *Visual* Multidimensional Geometry and its Applications

Alfred Inselberg

School of Mathematical Sciences, Tel Aviv University
aiisreal@post.tau.ac.il

With Parallel Coordinates the perceptual barrier imposed by our 3-dimensional habitation is breached enabling the visualization of multidimensional problems. The foundations are intuitively developed interlaced with applications and interactive demonstrations. A powerful knowledge discovery process enables the exploration of multivariate data with stunning results. The patterns representing relational information reveal properties, like convexity and non-orientability, of hypersurfaces unlocking new geometrical insights. Models of multivariate problems allow for the exploration of interrelations among parameters, sensitivities, tradeoffs and constraints for decision making. These patterns persist in the presence of errors and that is good news for the applications. We stand at the threshold of cracking the gridlock of multidimensionality. The parallel coordinates methodology is used in collision avoidance and conflict resolution algorithms for Air Traffic Control (3 patents), Computer Vision (patent), Data Mining (patent), optimization and process control.

Computer Algebra in Online STEM Education

C. James Cooper[1], Stephen M. Watt[2]

[1] *Maplesoft, Waterloo, Canada, cjcooper@maplesoft.com*
[2] *University of Waterloo, Canada, smwatt@uwaterloo.ca*

Maplesoft and the Faculty of Mathematics at the University of Waterloo have recently entered into a collaboration to produce a stream of online STEM courses based on the Möbius [1] platform. The Faculty of Mathematics already offers one completely online degree, the Master of Mathematics for Teachers, as well as online sections of many core courses. The Möbius platform is now being used to enhance the interactivity of online course assets and to allow fine-grained student evaluation. The present talk describes the main issues in developing the new online degrees.

References

[1] Maplesoft, *Online courseware environment that puts STEM first*, `http://www.maplesoft.com/products/Mobius/` (2016)

Jonathan Borwein: a PiONEER of Experimental Mathematics (Memorial lecture)

Doron Zeilberger

Rutgers University, USA

Jonathan Borwein was not only a great mathematician, he was a visionary who pioneered Experimental Mathematics, and was also very passionate about mathematical education.

New in the Wolfram Language - making Machine Learning and other modern computing disciplines easy to use

Erez Kaminski

July 6, 2017

Abstract

For the past 30 years the Wolfram Language, the language of Mathematica, has continued to evolve and reach new frontiers in computation and computer algebra. Alongside the continues development of well known attributes of the Wolfram Language (symbolic computation, equation solving, etc.), new features and disciplines have been introduced and made easy. Modern application of the language include Machine Learning, Image Processing, Server-less API calls, and much more. In this talk we will review these new features and show how to apply them to education and research, using the same easy to use syntax that made Mathematica so popular.

Free Students' Exercise Notebooks and Maple 2017 News

Omer Yagel

VP DigiSec, Israeli rep. of Maplesoft

Maple is known for its ease of use and user friendliness and the latest edition, Maple 2017, emphasising this point ever so. Maple 2017 has something new for everyone, whether it be an improvement to the ease of use of plots or an advanced mathematics feature.

At the outset of the presentation the Maple Tool Chain is fully exposed and some further emphasis is given to education related tools, such as Maple TA and the new Möbius project. After, the presentation gets into a more detailed survey of some of Maple 2017 new or improved features:

- Maple Workbook (2016)
- Maple Cloud
- Plot Builder
- New Plots, Plots annotation, Geographical information projection
- Password Protection
- New Data Types (2016)
- Improved Help

DigiSec is running an academic free content project for the benefit of the students community. A short demonstration would show how some of these new features are helping us in improving some of our existing content.

Session 1

Computer Algebra in Education

Session chairs:

Michel Beaudin
ETS, Montreal, Canada

Michael Wester
University of New Mexico, USA

Alkis Akritas
University of Thessaly, Greece

José Luis Galán García
Universidad de Malaga, Spain

Elena Varbanova
Technical University of Sofia, Bulgaria

Anatoli Kouropatov
Center for Educational Technology, Israel

Sara Hershkovitz
Center for Educational Technology, Israel

Using the Universal Math Environment Math-XPress for teaching and assessment of math courses Part I, Part II

P. Slobodsky[1], A. Ocheretovy[2], E. Roiz[3], A. Shtarkman[4]

[1] *Halomda Educational Software, Israel, halomda@netvision.net.il*
[2] *University of Ivanovo, Russia, alex_ocz@inbox.ru*
[3] *University of Ariel, Israel, roizevg@bezeqint.net*
[4] *Talpiot Teacher's College, Holon, Israel, anatoly@bezeqint.net*

In the talk we describe the main features of the Universal Math Environment Math-XPress and its use for classroom teaching, home training and assessment of math students at college and university levels. Math-Xpress includes linked modules of equation editor, 2D and 3D graph plotter, CAS expression evaluator and step-by-step solver, dynamic geometry (2D and 3D) and problem solving tutor.
Using the Problem Generator the courses in Calculus, Linear Algebra, Diff Equations, Statistics, Elementary Algebra, Geometry and others have been developed and used at Talpiot teacher's college and Ariel university regularly since 2007, involving thousands of students each academic year.

Part I

Math-Xpress the Universal Math Environment

The basic module of Math-XPress is *XPress-editor* - a graphical formula editor, enabling natural WYSIWYG editing of math expressions (Fig. 1), which can be either embedded into Word- or other format pages, or used by CAS based *XPress-evaluator, XPress-graph plotter* or *XPress-Tutor*.

$$\frac{1}{\varphi}=\frac{2}{\sqrt{5}+1}=\frac{2\left(\sqrt{5}-1\right)}{\left(\sqrt{5}+1\right)\left(\sqrt{5}-1\right)}=\frac{\sqrt{5}-1}{2}=\frac{\sqrt{5}+1}{2}-1=\varphi-1\rightarrow\ \frac{1}{\varphi}=\varphi-1$$

Fig. 1

Math-Xpress includes also two modules of interactive geometry: *2-D and 3-D XPress-geometry explorer*, which are in turn interrelated to other modules (Fig. 2). *XPress-graph plotter* enables plotting graphs of functions of 2 and 3 variables, families of functions and intersections of graphs (Fig. 3). *XPress-evaluator* performs algebraic operations in final form or step-by-step [1]. The subjects covered by *XPress-evaluator* include: Arithmetic, Elementary Algebra, Trigonometry, Calculus, Probability and Statistics, Linear Algebra, Complex numbers.

It enables to factorize polynomials, to solve equations and systems of equations and to perform most of algebraic operations step-by-step way, or to get numerical solution (Fig. 4).

Fig. 2

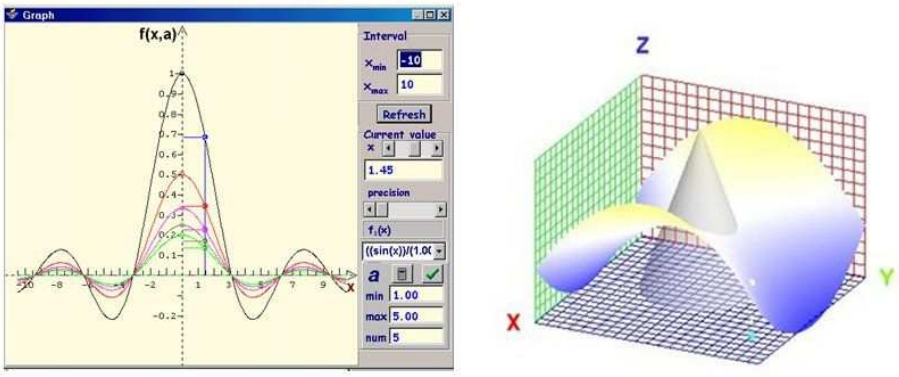


Fig. 3

All the objects created by *XPress-editor, Graph Plotter and Geometry Explorer* can be imbedded into Word or pdf-pages and called from them directly in interactive Math-Xpress environment. Closing the objects returns to the page from which they have been called.
This technology made it possible to develop fully interactive Math textbooks, first announced at [2] (`https://halomda.com/Maths-5.php`)

Part II

XPress-Tutor consists of content-based problems, presented in three modes: **Learning, Training** and **Test**. During a Learning mode, a student is offered a series of problems on a given subject; every problem includes randomly chosen parameters, so that different runs exhibit different initial sets of the parameters.

$$1\frac{3}{5}-7\frac{2}{9}=1-7+\frac{3}{5}-\frac{2}{9}=-6+\frac{3\cdot 9-2\cdot 5}{45}=-6+\frac{27-10}{45}=-6+\frac{17}{45}=-5\frac{28}{45}$$

$$\frac{2\cdot x}{1-3\cdot x}+\frac{4}{5\cdot x-6}$$

$$\frac{2\cdot x\cdot(5\cdot x-6)}{(1-3\cdot x)\cdot(5\cdot x-6)}+\frac{4\cdot(1-3\cdot x)}{(1-3\cdot x)\cdot(5\cdot x-6)}$$

$$\frac{2\cdot x\cdot(5\cdot x-6)+4\cdot(1-3\cdot x)}{(1-3\cdot x)\cdot(5\cdot x-6)}$$

$$\frac{10\cdot x^2-24\cdot x+4}{(1-3\cdot x)\cdot(5\cdot x-6)}$$

$$\frac{2\cdot\left(5\cdot x^2-12\cdot x+2\right)}{(1-3\cdot x)\cdot(5\cdot x-6)}$$

$$\frac{10\cdot x^2-24\cdot x+4}{(1-3\cdot x)\cdot(5\cdot x-6)}$$

$$\sqrt{x-1}+\sqrt{x+2}=3$$

$$2\cdot\sqrt{(x-1)\cdot(x+2)}+2\cdot x+1=9$$

$$2\cdot\sqrt{(x-1)\cdot(x+2)}=8-2\cdot x$$

$$4\cdot x^2+4\cdot x-8=4\cdot x^2-32\cdot x+64$$

$$36\cdot x=72$$

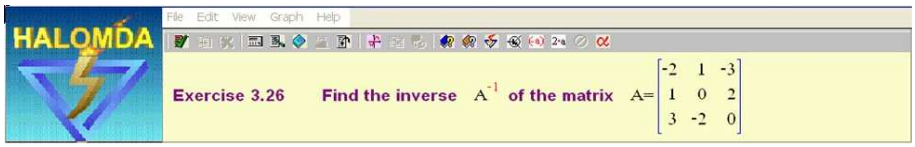
$$x=2$$

$$x_1=2$$

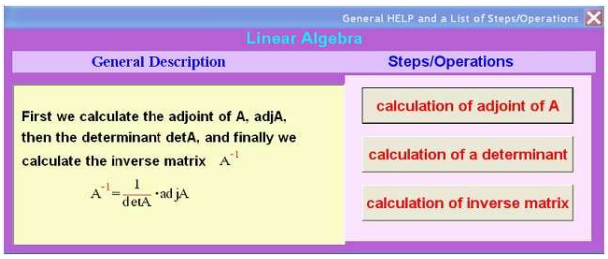
$$\sqrt{2-1}+\sqrt{2+2}=3$$

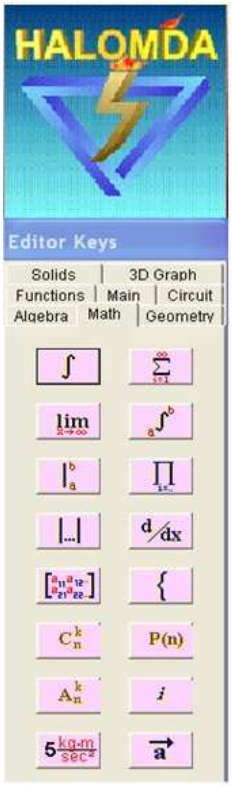
Fig. 4

A student may try solving a problem in his way, by entering an answer or an intermediate step of a solution. The program checks the input expression and responds. A student can also ask for a Help, that is presented in 3 levels:
1) A General Help, where a method of solution common to all the problems of a specific subject is described;
2) A List of Steps of a problem solution and the description of every step;
3) The Results of every Step of Solution (numerical or algebraic)
For the demonstration we consider the following example:

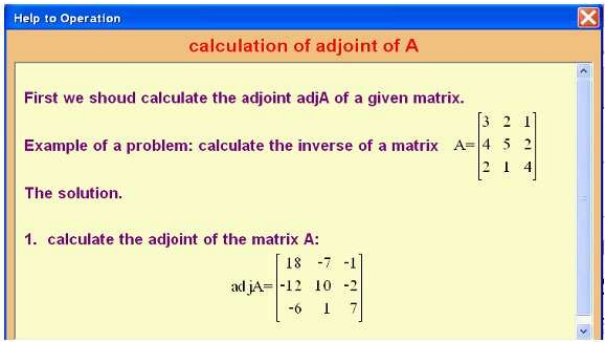


After trying to solve the problems a student can enter his result using the Editing Tools, or, pressing the Help key, he/she can call the Help window, where the General Method and a List of Solution Steps are presented:

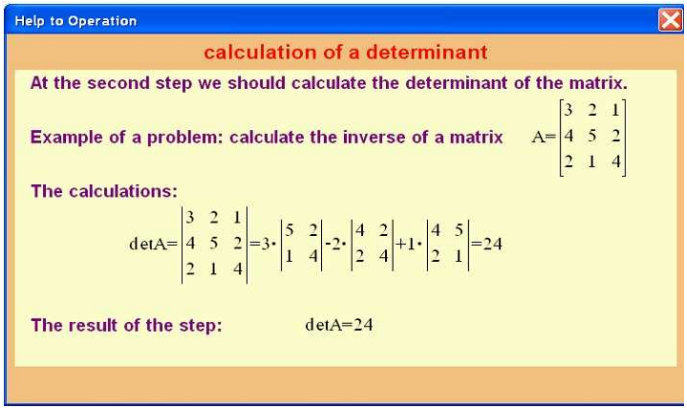




The General Method outlines the general ideas and methods that should be applied when solving a problem of a given type. By clicking the keys of solution steps, a student will see the detailed step-by-step solution of a problem similar to that offered to him/her (however, with different initial set of parameters).



After reading the description of a current step, the student is supposed to be able to implement it to the solution of the given problem. If, however, he/she still cannot get the correct result of the step, clicking on **Hint** shows the result. A student may wish to learn how to proceed with the solution, and call for the explanation of the second step:



After finishing all the steps, a student can either move to the next problem, or repeat the current one with a new initial data.

In **Training** mode, instead of viewing the result of every step when clicking **Hint**, a multiple choice of 4 possible results is presented, whereas in the **Test** mode, **no Help** is available, and a student solves the series of the problems as during the regular test.

In both Learning and Training modes **all the features of Math Xpress are available**, so that in a course of problem solving a student can explore the problem using different tools, that can help him/her in better understanding of a solution.

The problems are developed using the *XPress Problem Generator* external module, enabling compiling of new items by unexperienced in programming people [3].
During the last years thousands of problems have been developed covering the courses in Arithmetic, Elementary Algebra and Geometry for primary and intermediate schools, Algebra, Trigonometry and Introduction to Calculus for high schools, and Calculus, Linear Algebra, Differential Equations, Probability and Statistics for universities and colleges.
During the last academic year a course of Quantitative Thinking has been taught for 2 groups of students at Talpiot teacher's college, and all the courses on High Math have been used for teaching and intermediate exams for more than 3000 students at Ariel University.

References

[1] S.Kornstein, *Xpress Formula Editor and Symbolic Calculator*, Mathematics Teacher **94**, 5, p. 424 (2001).

[2] P.Slobodsky, *Computerized textbook in Physics and Math - a new approach to science education*, in *The Tenth International Conference on Technology and Education*, Cambridge, USA, pp. 25-26 (1993).

[3] P.Slobodsky, *Workshop on Integrated Computer Lessons in Physics and Mathematics developed on the basis of program generators "High Class", "Stages" and "Xpress"*, in *The 14 International Conference on Technology and Education*, Oslo, Norwegian, pp. 64-66 (1997).

Supporting Mathematical Thinking with CAS: The Need of Epistemic Change among Teachers.

Rotem Abdu

Levinsky College, Tel-Aviv, Israel

The current abundance of educational technologies, and computer algebra systems (CAS) in particular, carry a promise: new venues for advanced mathematical thinking. This promise is a product of teachers' ability to construct and simulate mathematical ideas that are dynamic and constrained by the mathematical world (represented with the CAS). This dynamic attribute is considered to bring a change in the way mathematical ideas are thought of: instead of prototypical examples that are drawn with pen and paper, CAS such as Geogebra can provide a dynamic context for inquiry of a full range of examples for mathematical concepts. Ultimately the goal is to create cohesive mental models of mathematical ideas.

The promise for new mathematical thinking afforded by CAS, however, is impeded by several factors. For example, Anthony and Clark, (2011) examine key factors that cause teachers to refrain from using CAS in their classrooms, including dilemmas of misalignment with other curricular goals and limited professional development. My interest in this talk, however, is in the change of epistemic stance that is required by teachers; from static prototypes to dynamic and invariant objects.

I will examine this point with a case study in which nine in-service teachers participated in an activity, in which they were asked to construct invariant models of mathematical objects — right triangle — with Geogebra. This activity was a part of a course on methodological issues in mathematics education. The teachers were familiar with Geogebra as part of their postgraduate curriculum. An analysis of the activity shows that the mathematical objects that were constructed by the teacher, at first, neglected the much necessary "invariance" attribute of such object: in the case of the right triangle created in Geogebra should stay a right triangle even if one of its vertices or segments is moved by the user. Upon instruction and refinement of the objective of the activity, teachers were gradually able to construct objects that are invariant. However, the idea of invariance became what Cobb et al., (2001) would call "a socio-mathematical norm" among the teachers, only after two more similar activities.

I conclude that there is a need for epistemic change — even among teachers that are supposedly familiar with Geogebra — from seeing CAS as tools that afford static prototypes to seeing them as environments for building and simulating invariant-dynamic objects. For that matter, teachers need to participate in activities that would provide them with opportunities to make that epistemic change;

namely, they should be engaged in building such models as well as observing other who do so. These results has also carry a nesting effect: if a teacher is not familiar with the invariant principle, there are good chances that their students will not adopt this epistemic stance either. Moreover, the illustrated case also suggest that "frontal" teaching with CAS — without students' or teachers' hands-on experience and building of objects — will yield limited learning in terms of achieving advanced mathematical thinking.

References

[1] Anthony, A. B. and Clark, L. M., *Examining dilemmas of practice associated with the integration of technology into mathematics classrooms serving urban students*, *Urban Education*, **46**(6), 1300–1331 (2011).

[2] Cobb, P., Stephan, M., McClain, K., and Gravemeijer, K., *Participating in classroom mathematical practices*, In *A journey in mathematics education research* (pp. 117–163), Springer Netherlands (2010).

Active learning in High-School mathematics using Interactive Interfaces

E.S. Cheb-Terrab[1], K. von Bülow[1]

[1] *Maplesoft R&D, Canada, ecterrab@maplesoft.ca*

The key idea in this project is to learn through exploration using a web of user-friendly Highly Interactive Graphical Interfaces (HIGI). The HIGIs, structured as trees of interlinked windows, present concepts using a minimal amount of text while maximizing the possibility of visual and analytic exploration. These interfaces run computer algebra software in the background. Assessment tools are integrated into the learning experience both within the HIGIs and at a general conceptual map, the *Navigator* level. The Navigator offers students self-assessment tools and full access to the logical sequencing of course concepts, helping them to identify any gaps in their knowledge and to launch the corresponding learning interfaces. An interactive online set of HIGIS of this kind can be used at school, at home, in distance education, and both individually and in a group.

References

[1] K. von Bülow, E. S. Cheb-Terrab and D. Teixeira Alves, *Edukanet Interactive mathematical Software*, Adv. Math. *The Lornet 2007 Conference on "User Centered Knowledge Environments: from theory to practice"* (Lornet-2007), Montreal, Canada, (2007).

Dynamic Computer Illustrations and Didactic Considerations in the Learning and Teaching of Mathematics

Michal Fraenkel[1]

[1] *Center for Educational Technology, Israel*

Years ago, as a math teacher, I used to dream of a dynamic way to show my studen ts mathematical concepts and situations, such as rotating graphs around a rotati on axis, graphs of functions changing according to the change of parameters, the range of different situations meeting a certain set of data, etc.

This is no longer a dream — the tools are already here: We have dynamic software that opens for us thousands of new ways to show our students this fascinating world called "mathematics" — alongside which arise thousands of new questions.

How does the use of dynamic computer illustrations affect users' way of thinking ? How does it affect the way teachers think? The way students think? If using dy namic illustrations has any disadvantages, what may they be?

In my talk, I will show various Geogebra illustrations developed for high-school students. I'll discuss different aspects of using them and offer possible considerations concerning questions such as:

- When should we use a dynamic illustration, and when should we avoid it?
- Should the students' age and level of the class be taken into account when considering the use of dynamic computer illustrations?
- What other considerations may help a teacher decide whether or not to use a dynamic computer illustration?
- Once a teacher decides to use a dynamic computer illustration, what considerations should he or she take into account while actually using it in their classroom?
- What considerations should be taken into account while developing dynamic computer illustrations?

Activities in Geometry built with GeoGebra around traditional Jewish artifacts

Th. Dana-Picard[1], S. Hershkovitz[2]

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

[2] *Center for Educational Technology, Tel Aviv, Israel, sarah@cet.ac.il*

Traditional Jewish artifacts show different kinds of symmetries: rotational symmetry, axial symmetry, sometimes translations (e.g. in architecture). Other affine plane transformations may appear, such as affinities (see [1]).

The study of these geometrical features may be a basis for courses in plane and space geometry and in analytic geometry. This has been the basis for mathematical activities for a population of students coming from the so-called orthodox population in Israel. Until their arrival to pre-academic programs and then to undergraduate studies, these students have studied previously only Talmudic studies, therefore the usage of artifacts form their natural environment helps to draw their attention.

This symbiosis is the basis of various works in Mathematics Education. Moreover, the usage of technology helps the students to find their own experimental way to acquire more mathematical knowledge, the technological skills being part of this new knowledge. This has been used a couple of years ago for a course on Analytic Geometry both for pre-service and for in-service teachers (see [3]).

We are currently experimenting this framework both for high-school students and for undergraduate students. This fits the official syllabus. The main technological tool used in these courses is GeoGebra.

In our talk we will describe an activity built around architectural motives, and show how students used GeoGebra to build a model, by enhancing knowledge in Analytic Geometry. If some students use the DGS only as a plotter, many students use mathematical knowledge (equations of lines, plane geometry, rotations and axial symmetries) to program their work with the software, plotting a minimal number of elements and reproducing them using plane transformations. We present three different approaches for the mind-and-machine interaction.

We wish to mention that this work is part of an ongoing ERASMUS project on STEAM education headed by Metropolitan University, Budapest.

References

[1] Th. Dana-Picard and S. Hershkovitz (2017): *A Glimpse at Mathematics in Jewish Traditional Artefacts*, to appear in the Symmetry Journal.

[2] Yu Manin (2015): *Mathematics, Art, Civilization*, in Art in the Life of Mathematicians (Anna Kepes Szemeredi, edt), American Mathematical Society, RI: Providence, 168-186.

[3] N. Zehavi, R. Zaks and Th. Dana-Picard (2006): *Analytic Geometry, Computer Assisted Activities*, Teachers resource e-book, Machshevatika, Department of Science Teaching, Weizmann Institute, Rehovot.

Dynamic Geometry Software Supplemented with Computer Algebra as a proving tool

R. Hašek

University of South Bohemia in České Budějovice, Czech Republic, hasek@pf.jcu.cz

The topic of this contribution is aimed at lower and upper secondary school mathematics teaching as well as at university training of teachers of mathematics.

Joint use of computer algebra (CAS) and dynamic geometry software (DGS) or even an incorporation of CAS into DGS brings new possibilities into the teaching of mathematics, such as experimentation, the modelling of real-world situations or deriving and proving of hypotheses [3, 4, 5]. We will deal particularly with the latter issue of proving, namely with the question of the use of DGS and CAS as a means of finding a proof. While the positive role of a proof in mathematics teaching and learning is obvious [2], the beneficial use of computers to find a proof suitable for teaching still requires detailed research. Also, among others, in connection with the actual integration of algorithms of the automated theorem proving into DGS [1]. First, we will briefly present up to date findings of such research. Then, through specific examples, coming from secondary school mathematics or teacher training courses, we will introduce several possible ways of using computer algebra and dynamic geometry when dealing with proofs in mathematics teaching.

References

[1] F. Botana, M. Hohenwarter, P. Janičič, Z. Kovács, I. Petrovič, T. Recio and S. Weitzhofer, *Automated Theorem Proving in GeoGebra: Current Achievements*, Journal of Automated Reasoning, **55**(1), pp. 39-59 (2015).

[2] G. Hanna and de M. Villiers (Eds.), *Proof and proving in mathematics education: the 19th ICMI study*. Dordrecht: Springer, (2011).

[3] R. Hašek, *Investigation of logarithmic spirals in nature by means of dynamic geometry and computer algebra systems* [Online], The Electronic Journal Of Mathematics And Technology, **6**(3), pp. 216-230 (2012). Available at `https://php.radford.edu/~ejmt/ContentIndex.php#v6n3`

[4] R. Hašek, *Systems of Computer Algebra and Dynamic Geometry as Tools of Mathematical Investigation*, The International Journal For Technology In Mathematics Education, **20**(3), pp. 103-108 (2013).

[5] R. Hašek and J. Zahradník, *Study of historical geometric problems by means of CAS and DGS*, The International Journal for Technology in Mathematics Education, **22**(2), pp. 53-58 (2015).

Geometric constructions problems in dynamic environment: new elegance and new dilemmas in teacher training

I. Sinitsky[1]

[1] *Gordon College of Education, Haifa, Israel, sinitzsk@gordon.ac.il*

After almost two decades of ignoring the issue of construction with straightedge and compass in Israeli high school curricula, they came back to textbooks together with technologies and interactive geometry software (IGS). The IGS offers students to discover the properties of geometric objects in the style of inquiry as a process of problem posing and problem solving. The presentation discusses horizons and dilemmas of using dynamic geometry environment for solutions of construction problems in teacher training. Among didactic dilemmas we mention the existing of 'non-classic' tools of GeoGebra with allow almost immediate solutions of some 'difficult' construction problems (for example, three circles Appolonius problem), and the students' use of built-in tools for simple geometric constructions. Concerning straightedge-and-compass construction problems, we suggest the approach based on using the idea of interplay of change and invariance [1, 2]. This approach provides the solution in the manner that fits the typical way of reasoning of students. Since they have a difficulty to build geometrical object that simultaneously satisfies different requirements, we suggest to split a whole problem into multiple stages with the single construction demand at each one. Technically, the approach use tracing as a tool to discover a hidden invariant and to construct a suitable change. The approach is illustrated with solutions of constructions problems that involve different transformations of intermediate object: translation, homothety and others.

References

[1] I. Sinitsky and B. Ilany, *Change and Invariance. A textbook on Algebraic Insight into Numbers and Shapes.*, Sense Publishers, Rotterdam/Boston/Taipei (2016).

[2] I. Sinitsky and M. Stupel, *Invariants in geometry: a long-term history and current implications for learning.*, Levenberg, I.& Patkin, D.(eds.), The many aspects of geometry - From research to practice in geometry teaching. nd ed., MOFET, (2017, in Hebrew).

Searching for loci using DGS and CAS

J. Blažek[1], P. Pech[2]

[1] *University of South Bohemia, Czech Republic, blazej02@pf.jcu.cz*
[2] *University of South Bohemia, Czech Republic, pech@pf.jcu.cz*

Searching for geometric loci belongs to the traditional part of mathematics school curricula all over the world. This topic is generally considered to be quite difficult for students, despite many well–known loci are around us, such as lines, circles or conics.

Nowadays new computational technologies substantially facilitate investigation of loci, especially in a plane. Dynamic geometry software such as Cabri, GeoGebra, Sketchpad and others offer several methods how to describe the locus. The use of this software enables to draw the desired locus and mostly to obtain its locus equation. The use of a new GeoGebra command LocusEquation which provides an analytic description of the sought locus based on the theory of automated theorem proving is presented.

In the talk a few examples which are accompanied with possible solutions and comments are given.

By searching for the locus we will apply Groebner bases and Wu–Ritt methods using software CoCoA[1] and Epsilon library[2].

References

[1] Abánades, M. A., Botana, F., Montes, A., Recio, T.: An algebraic taxonomy for locus computation in dynamic geometry. Computer-Aided Design 56, 2014, 22-33.

[2] Capani, A., Niesi, G., Robbiano, L.: CoCoA, a System for Doing Computations in Commutative Algebra. `http://cocoa.dima.unige.it`

[3] Chou, S. C.: Mechanical Geometry Theorem Proving. D. Reidel Publishing Company, Dordrecht, 1987.

[4] Roanes–Lozano, E., Roanes–Macías, E.: Automatic Determination of Geometric Loci. 3D-Extension of Simson–Steiner Theorem, in: Lecture Notes in Artificial Intelligence, 1930, AISC 2000, pp. 157-173.

[5] Shikin, E., V.: Handbook and Atlas of Curves. CRC Press, Boca Raton, 1995.

[6] Wang, D.: Epsilon: A library of software tools for polynomial elimination, in: Mathematical Software, (Cohen, A., Gao, X. S., Takayama, N., eds). World Scientific, Singapore New Jersey, 2002, pp. 379–389. `http://www-calfor.lip6.fr/~wang/epsilon/`

[7] Wang, D.: Elimination Practice. Software Tools and Applications. Imperial College Press, London, 2004.

[1] Program CoCoA is freely distributed at `http://cocoa.dima.unige.it`

[2] Program Epsilon is freely distributed at `http://www-calfor.lip6.fr/~wang/epsilon/`

Checking solutions of tasks on expressibility in Boolean algebra of sets

R. Prank

University of Tartu, Estonia, rein.prank@ut.ee

The paper describes some steps in a trial to computerize a new type of exercises in Predicate Logic. Many introductory courses contain exercises on expression of predicates using first order formulas in some given signature of constant, functional and predicate symbols. Most exploited mathematical topic is here arithmetic of natural numbers using signature $\langle\ 0\ ;\ ',+,\cdot\ ;=\rangle$ (or similar). For example,
"x is even", "$x/y=z$" and "$x\leq y$ are quite easy tasks but "x is prime" or
"x is greatest common divisor of y and z" are harder for students.

In this paper we consider another quite reasonable exercise topic - predicates defined on subsets of a fixed set, for example of set of natural numbers N. Books on Boolean algebras or lattices show how the elementary statements of these theories can be formulated in the signature of Boolean operations $\langle\ ',\cap,\cup\ ;=\rangle$ or in the signature of order relation $\langle\subseteq\rangle$. For example,

$$X\subseteq Y\Leftrightarrow X\cup Y=Y, \tag{1}$$

$$X\cup Y=Z\Leftrightarrow(X\subseteq Z)\wedge(Y\subseteq Z)\wedge\forall W[(X\subseteq W)\wedge(Y\subseteq W)\rightarrow(Z\subseteq W)]. \tag{2}$$

In our course we use both signatures for expression of predicates like
"$X=Y$", "$X=\emptyset$", "$X'=Y$", "$X\setminus Y=Z$", "$|X|=m$" but also for their combinations:
"$X\cap(Y\cup Z)=W$" or "X is union of Y and some 2-element set".

The weaker students compose often wrong answers to expressibility tasks. It would be desirable to create a computerized solution environment. Existing general-purpose methods of expression handling enable detection of (quite frequent) technical errors: incorrect syntax, superfluous or missing free variables, using symbols that do not belong to the required signature, confusion of set-theoretic expressions and formulas. But the main problem is checking of correctness of answer. Correctness of answer of expressibility tasks means equivalence with the 'correct' formula. For arithmetic of natural numbers, equivalence of first order formulas is undecidable. For being able to evaluate student answers, the Tarski's World [1] uses exercises with predicates on finite domains. For the class of all Boolean algebras and also for any particular Boolean algebra the problem of equivalence is decidable [2, 3]. In our project we investigate the question whether the equivalence (in algebra $P(N)$) can be checked sufficiently quickly.

The following propositions describe what defines the truth-value of formulas of the signature $\sigma = \langle\ \emptyset;\ ',\cap,\cup\ ;=\rangle$. For sets $X_1,...,X_n$ let $\pi_i(X_1,...,X_n)$ denote their "Venn intersections" $X_1 \cap ... \cap X_n,\ ...,\ X_1' \cap ... \cap X_n'$ (where $1 \le i \le 2^n$).

Propositon 1. Let $F(X_1,...,X_n)$ be any quantifier-free formula with free variables $X_1,...,X_n$ in signature σ. If $A_1,...,A_n$ and $B_1,...,B_n$ are collections of sets having equal Venn diagrams, i.e.
$\pi_i(A_1,...,A_n) = \emptyset \Leftrightarrow \pi_i(B_1,...,B_n) = \emptyset \qquad (1 \le i \le 2^n)$.
Then $\qquad F(A_1,...,A_n) = t \Leftrightarrow F(B_1,...,B_n) = t$.

Quantified formulas enable describe also finite cardinalities of sets. For $1 \le i \le 2^n$ we have
$|A| = m \Leftrightarrow \exists Y_1 ... \exists Y_n (A \cap \pi_1(Y_1,...,Y_n) \ne \emptyset \wedge ... \wedge A \cap \pi_m(Y_1,...,Y_n) \ne \emptyset) \wedge$
$\neg \exists Y_1 ... \exists Y_n (A \cap \pi_1(Y_1,...,Y_n) \ne \emptyset \wedge ... \wedge A \cap \pi_{m+1}(Y_1,...,Y_n) \ne \emptyset)$.

The following proposition tells that the only expressible predicates are combinations of cardinalities of regions of Venn diagrams.

Propositon 2. Let $G(X_1,...,X_n)$ be any formula of signature σ that does not contain other free variables beside $X_1,...,X_n$ and where the maximal number of nested quantifiers is k. If $A_1,...,A_n$ and $B_1,...,B_n$ are such collections of sets that for every i (where $1 \le i \le 2^n$) the following holds:
1) $|\pi_i(A_1,...,A_n)| \ge 2^k \Leftrightarrow |\pi_i(B_1,...,B_n)| \ge 2^k$
2) if $\quad |\pi_i(A_1,...,A_n)| < 2^k \quad$ then $\quad |\pi_i(A_1,...,A_n)| = |\pi_i(B_1,...,B_n)|$.
Then $\quad G(A_1,...,A_n) = t \Leftrightarrow G(B_1,...,B_n) = t$.

Corollary. For characterization of any formula it is sufficient to find its truth-values for all combinations of cardinalities $0,...,2^k$ of regions of Venn diagram of the free variables.

If the formula has n free variables and maximal number of nested quantifiers is k then the Venn diagram contains 2^n regions and we should examine $2^k + 1$ possible cardinalities for each region i.e. our 'extended column' of truth-values contains $(2^k + 1)^{2^n}$ bits. Numbers of necessary truth-values are presented in the following table:

Table 1. Free variables, nested quantifiers and numbers of truth-values

k (nested quantifiers) / **n (free variables)**	**0**	**1**	**2**	**3**	**4**
1	4	9	25	81	289
2	16	81	625	6561	83521
3	256	6561	390625	43046721	
4	65536	43046721			

Most of 'elementary' predicates in usual student exercises have 1-3 arguments. Bigger numbers appear when we express composite predicates. Typical examples are here predicates describing combined set-theoretical expressions like $(X \cup Y) \cap Z = W$ but also $X \setminus Y = Z$. They require in signature $\langle \subseteq \rangle$ formulas with 4+2 and 3+3 variables. In case of algebraic signature the formulas are less complex and this allows also simplifying of internal representations. At the moment of composing the abstract we work on calculation of cases 4+1 and 3+3 for acceptable time.

Fortunately the natural solution strategy of expressibility tasks is not immediate input of the final formula. Already in paper-and-pencil technology we recommend the students to solve tasks step by step building some intermediate predicates. In computer environment we can predict this approach more efficiently, proposing appropriate choice of intermediate predicates (we can also allow substitution of formulas from earlier tasks). This way allows also checking the intermediate formulas step by step and reducing the number of nested quantifiers.

What kinds of feedback can be provided, using our computing engine? First the program can use traditional methods for checking the syntax, free variables, usage of signature symbols and expressions of correct type. Next, the described above technical reasons enforce the program to reject the formulas that are too complex (contain too much nested quantifiers). After that the main loop of the program counts the truth-values of etalon formula and student formula for all cardinality cases from the Proposition 2. If some distribution of cardinalities of regions of Venn diagram gives a wrong truth-value then the program can use these cardinalities for building a concrete example of sets where the formula fails. For example, if the student enters for the predicate $X \cup Y = Z$ the formula $(X \subseteq Z) \wedge (Y \subseteq Z)$ instead of formula (2) then the program can respond with the simplest counterexample $X = \emptyset, Y = \emptyset, Z = \{0\}$.

References

[1] J. Barwise and J. Etchemendy, *Language, Proof and Logic*, Stanford : CSLI Publications, (2007).

[2] A. Tarski, *Arithmetical classes and types of Boolean algebras*, Bull. Amer. Math. Soc., **55**, pp. 64 (1949).

[3] Yu. Ershov, *Decidability of the elementary theory of relatively complemented distributive lattices and of the theory of filters*, Algebra i Logica, **3**, 3, pp. 17-38 (1964) (Russian).

Constructing Rational Gram–Schmidt Problems and QR Problems

David J. Jeffrey and Nasir Khattak

Dept Applied Mathematics & ORCCA, University of Western Ontario, Canada, djeffrey@uwo.ca

A standard topic in Linear Algebra is the Gram-Schmidt process. It is equivalent to obtaining the *QR* factoring of a matrix. When books use the name Gram-Schmidt, they start with a set of vectors; when they use the term *QR* decomposition, they start with a matrix. They are equivalent because each matrix column is a vector. The aim in either case is to make each column of unit length, in the 2-norm, and also make each column orthogonal to all others. The resulting matrix is called orthonormal (or orthogonal). So a matrix A is factored (decomposed) as

$$A = QR\,,$$

where Q is orthonormal and R is upper triangular, and Q has the property that $Q^TQ = I$, that is, its inverse equals its transpose. In *numerical* linear algebra, an important property is that Q can be regarded a rotation matrix, and therefore it does not amplify rounding errors the way that *LU* factoring does. The 2-norm is the square-root of the sum of squares of the components of a vector, and hence the Gram-Schmidt process includes many square-roots, which make exam questions painful, because the students get lost. How nice if all square roots were exact!

We all know $3^2+4^2=5^2$ (don't we); so the 2-norm of vector $[3,4]$ is 5. Some may know that $3^2+4^2+12^2=13^2$; so the 2-norm of $[3,4,12]$ is 13. We can use this to construct matrices with rational *QR* factors.

In general, we define a *pythagorean n-tuple* by the equation

$$x_1^2+x_2^2+\ldots+x_{n-1}^2=x_n^2\,,$$

where the x_k are all integers. Then the above examples are a pythagorean triple and quadruple. A number of algorithms have been published to generate n-tuples [1], but we need *orthogonal* n-tuples. At the moment, the only way we have found to get the orthogonality property is brute force (exactly what computer algebra is good at). However, it works quite well, and we have successfully constructed 5-by-5 matrices with rational *QR* factors.

References

[1] Sophie Frisch & Leonid Vaserstein, *Polynomial parametrization of Pythagorean quadruples, quintuples and sextuples*, J. Pure Applied Algebra **216**, pp. 184–191 (2011).

How to Use CAS (Maple) to Help Students Learn Number Theory

M. Durcheva[1]

[1] *Technical University of Sofia, Bulgaria, {mdurcheva66}@gmail.com*

At the Technical University of Sofia (TUS), some topics of Number Theory are taught in the "Discrete mathematics" course. The notions of the Number Theory are very important for the students of computer sciences, as they are necessary, for instance, for the "Cryptography" course.

As it is pointed out in [1], for an effective mathematical education it is useful the teacher to:

- challenge his students to think deeply about the problems they are solving;
- influence learning by posing challenging and interesting questions;
- encourage students' ability to "do" mathematics.

This paper will highlight some successful strategies for enhancing students' learning that the author has used in teaching topics of Number Theory at the TUS. In particular, the use of the CAS (Maple) expands students' ability to "do" mathematics and to reach beyond the solutions and algorithms required to solve the problem.

There are some problems in Number Theory where we can apply CAS in proving a statement, as it is in the

Problem 1. Prove that for all prime p, the number $p^{2017}-1$ is a composite.

It is clear that for all odd primes the proposition is obviously true. It remains, students using CAS, to check it for $p=2$.

Another approach we use to influence students' learning, is to pose concrete small problems and to ask students to make a hypothesis and then to prove it.

Problem 2. a) Check whether the numbers $x=3^{2016}+2^{2018}$ and $y=2017^4+4^{2017}$, are primes.

b) Factorize $z=2^{4n+2}+1$.

c) Find the general form of x, y, and z, and try to make a conclusion.

Maple gives the factorization of the general form a^4+4b^4.

Another interesting types of numbers are Fermat numbers. To introduce the properties of these numbers to the students, the teacher could include the following

Problem 3. a) Check whether the numbers of the type $2^{2^n}+1$ are primes.

b) Find the last digit of their decimal representation for $n \geq 2$.

For 3,b, CAS helps students to make a conjecture and then most of them attempt to prove it on their own.

Because there are some theorems in Number Theory, whose proofs are very complicated or rely on advanced mathematics, it is useful students "to be convinced" in their truthfulness, as in the

Prime number theorem. [2, 3] The function $\pi(x)$ ($\pi(x)$ is the number of primes $\leq x$) is asymptotic to $x/\ln(x)$, in the sense that

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

At the TUS, Number Theory is taught in the first year, so we do not include the proof of the this theorem in our course. That is way, it is very important for us to motivate students to observe the truthfulness of the Prime number theorem. Maple can help the teacher significantly in this direction. The teacher may pose the following

Problem 4. Graph on the same plot the graphs of the functions $\pi(x)$ and $x/\ln(x)$. Make a conclusion.

Another approach to enhance students' learning is to pose them challenging questions that not only stimulate students' innate curiosity, but also encourages them to investigate further. For instance, when studying numerical function $\tau(n)$, the teacher can ask the following

Problem 5. Study the function $\tau(n)$ (using Maple). What conjectures can you make about it? Is there a formula for $\tau(n)$? Is the function $\tau(n)$ multiplicative?

One of the most difficult topics in Number theory are **Diophant equations**. However, using Maple, some kind of linear Diophant equations can be easily solved. Here the teacher could pose intriguing problems to motivate students to study this topic.

While we are not in a position to run a controlled experiment to prove the efficiency of these teaching methods, there have been several benefits in our classroom. The students are more engaged, more likely to try to solve the problems on their own, and at the end, they score higher on examinations.

References

[1] N. Protheroe, *What Does Good Math Instruction Look Like?*, Principal **7**, 1, pp. 51-54 (2007).

[2] K. Rosen, *Elementary Number Theory and lts Applications*, Addison-Wesley Publishing Company (1986).

[3] N. Obreshkov, *Number Theory*, University Publishing House "St. Kl. Ohridski" (2004) (in Bulgarian).

Using Maple cloud computing in financial education of pre-service teachers

V. Petrášková[1], P. Rosa[2]

[1] *University of South Bohemia, Czech Republic, petrasek@pf.jcu.cz*
[2] *University of South Bohemia, Czech Republic, rosapr00@pf.jcu.cz*

The presentation deals with an original collection of educational materials developed by the authors at the Faculty of Education at the University of South Bohemia. Main goal of these materials is to support the financial education of future teachers with interactive environment in addition to the usual computer means of financial computation such as spreadsheet and online calculators. Maple enables to create interactive documents whose interactivity consists in implementation of a simple user interface beyond the framework of usual document. This fact enables the user to influence the computation result by a change in input parameters and thus de facto to simulate an inexhaustible number of situations.

Reference

[1] H. Binterová and P. Tlustý, *Digital Learning Environment for Mathematics*, in *Proceedings of the 10th International Conference on Efficiency and Responsibility in Education* (ERIE 2013), Czech University of Life Sciences, Prague, pp. 611-617 (2013).

[2] R. Hašek and V. Petrášková, *Issue of Financial Capability*, The International Journal for Technology in Mathematics Education, **17**, 4, pp. 183-190 (2009a).

[3] R. Hašek and V. Petrášková, *Effective methods of teaching financial issues*, in *Proceedings of the 11th International Conference Efficeency and Responsibility in Education*, (ERIE 2014), Czech University of Life Sciences, Prague, pp. 186-192 (2014).

[4] R. Hašek and V. Petrášková, *Financial Education in Teacher Training with Technological Support*, International Handbook of Financial Literacy, Springer Science+Business Media Singapore, Singapore, pp. 675-696 (2016).

[5] A. Lusardi, O. Mitchell and V. Curto, *Financial literacy among the young*, The Journal of Consumer Affairs, **44**, 2, pp. 358-380 (2010).

[6] V. Petrášková, *Pre-service mathematics Teachers' Financial Literacy*, The New Educational Review, **34**, 4, Wydawnictwo Adam Marszalek, Torún, pp. 280-291 (2013).

[7] R. Hašek and V. Petrášková, *Cesta ke zvyšování finanční gramotnosti*, e- Pedagogium, Univerzita Palackého v Olomouci, Olomouc, pp. 86-107 (2009b).

[8] A. Hošpesová and V. Petrášková, *Beginning with financial literacy on primary school level?*, SEMPT 2013 - International Symposium Elementary Mathematics Teaching. Proceedings – Tasks and Tools in Elementary Mathematics, Praha, pp. 351-353 (2013).

[9] E. Wuttke, et.al., International Handbook of Financial Literacy, Springer, Berlin (2016).

Some examples of solving nonlinear programming problems with CAS

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

We would like to present some examples of solving nonlinear programming problems using Mathematica and wxMaxima. It's a didactic proposal to support teaching students nonlinear programming (NLP) using CAS. Elements of NLP are taught in the framework of such university courses as for example: mathematical analysis, mathematical programming, operation researches or optimization methods. In the framework of this talk we will present graphical method (dynamic plots) for solving integer NLP, NLP problems, several examples for Karush-Kuhn-Tucker conditions and two examples for convex optimization. We will consider NLP problems in the following form:

$$\begin{aligned} \underset{(x_1,x_2,\ldots x_n)}{\text{maximize}} \quad & f(x_1,x_2,\ldots,x_n) \\ \text{subject to:} \quad & g_i(x_1,x_2,\ldots,x_n) \geq 0,\ i=1,2,\ldots m, \\ & (x_1,x_2,\ldots,x_n) \in X, \end{aligned}$$

where n and m are positive integers, X is a subset of $\mathbb{R}^n$ and f, g_i are real-valued functions on X with at least one function of f, g_i $(i = 1,2,\ldots,m)$ being nonlinear.

References

[1] S. M. Bazaraa and C. M. Shetty, *Nonlinear programming. Theory and algorithms.*, John Wiley and Sons, (1979)

[2] Adam Ostaszewski, *Advanced Mathematical Methods (London School of Economics Mathematics).* Cambridge University Press; 1 edition (January 25, 1991)

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

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

Engineering Mathematics and CAS

Michel Beaudin[1]

[1] *École de technologie supérieure (Canada), michel.beaudin@etsmtl.ca*

The computer algebra system TI- Nspire CX CAS will be used to show how some mathema-tical results can be illustrated by a CAS. The talk will make interesting connections between subjects that seem to be different.

The first example will be about odd, even and periodic functions. Beginning engineering students have problems to clearly understand the concept of even functions, odd functions and -much more seriously- the concept of inverse functions. We think the graphical capabilities of Nspire can be used to overcome this problem. The graphic editor of Nspire CAS will guide us to extend functions that are first defined over an interval on one side of the origin: extensions will be even or odd ones. Then the modulo function will be used to extend it periodically. In the case of inverse functions, the important fact is the concept of one to one function and the restriction of the domain of a given function. We will be able to do this very easily because Nspire CAS has nice templates to do such operations.

In the second example, we will use the modulo function and the D'Alembert's solution to solve the one dimensional wave equation in the case of zero initial velocity. We will recall the series solution of this problem, based on the method of separation of variables. Then, the solution will be obtained, using the sum of two opposite waves. If, in addition, we take zero initial velocity, then the solution can be shown to simplify into an odd periodic function: this is where the modulo function will act and an easy animation will be possible and performed. The big advantage over the series solution is trivial: no need to take a partial sum to plot the graph because the infinite series has been simplified into a closed-form.

Finally, we will move to Fourier series in order to connect these two examples. We showed at ACA 2013 how to define a Fourier function in Nspire CAS able to do exactly what the good old Derive software Fourier function is doing. Being able to plot the graph of any periodic function, we will find its Fourier partial sum and plot both graphs on the same window.

Future engineers at our engineering school are not so different from the ones in other parts of the world: they use mathematics as a tool. If they want to be able to *see* rapidly the results of a computation, their portable TI-Nspire CX CAS handheld does the job in the classroom and during exams. Of course, outside the classroom or during a regular course, the software version of Nspire is a more convenient choice.

Generating Power Summation Formulas Using a Computer Algebra System

Michael Xue[1]

[1] *Vroom Laboratory for Advanced Computing, USA, mxue@vroomlab.com*

Mathematical induction is often used in classroom to *prove* various Power Summation Formulas such as

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \tag{1}$$

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} \tag{2}$$

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4} \tag{3}$$

However, how the formulas are obtained in the first place is rarely discussed.

In this presentation, we will *construct* the Power Summation Formulas. Specifically, a recursive algorithm is derived and its implementation in Computer Algebra generates the formulas. A closer look at this algorithm also reveals the generated formulas can also be obtained by solving an initial-value problem of difference equation symbolically.

References

[1] J. Gullberg, *Mathematics From the Birth of Numbers* (1997).

[2] *Omega: A Computer Algebra System Explorer*, at http://www.omega-math.com

A `sympy/sage` Module for Computing Polynomial Remainder Sequences

Alkiviadis G. Akritas* Gennadi I. Malaschonok† Panagiotis S. Vigklas‡

March 2, 2017

Extended Abstract

Given the polynomials $f, g \in \mathbb{Z}[x]$, we are interested in the following four polynomial remainder sequences (prs's):

(a) Euclidean prs,

(b) Modified Euclidean prs,

(c) Subresultant prs, and

(d) Modified Subresultant prs.

The Modified Euclidean prs is obtained by modifying the sign of the remainder of each polynomial division performed for the computation of the Euclidean prs. Analogously, the Modified Subresultant prs is obtained by modifying the matrix from which the Subresultant prs is obtained.

Even though prs's (c) and (d) are computed by evaluating sub-determinants of given matrices, our objective is to compute *all four prs's* using the *same* type of polynomial divisions over the ring $\mathbb{Z}[\mathrm{x}]$.

Our objective is not at all trivial and has eluded the efforts of great mathematicians, as our brief review below indicates.

Initially, Collins, Brown and Traub [8], [9], [11], [12] used the so called `prem` pseudo-remainder function defined by

$$\mathrm{LC}(g)^{\delta} \cdot f = q \cdot g + h, \tag{1}$$

where $\mathrm{LC}(g)$ is the leading coefficient of the divisor g, and

$$\delta = \mathrm{degree}(f) - \mathrm{degree}(g) + 1. \tag{2}$$

*Department of Electrical and Computer Engineering, University of Thessaly, GR-38221, Volos, Greece, Tel.: +30 242110 74886, Fax: +30 24210 74997, akritas@uth.gr

†Laboratory for Algebraic Computations, Tambov State University Internatsionalnaya, 33, RU-392000 Tambov, Russia, malaschonok@gmail.com

‡Department of Electrical and Computer Engineering, University of Thessaly, GR-38221, Volos, Greece, pviglas@uth.gr

However, using `prem` *only* the signs of prs (c) can be *exactly* computed ([10], pp. 277–283). The signs of the other three prs's, (a), (b) and (d), *may* not be exactly computed when the prs is *incomplete*, i.e. when there are gaps in the degree sequence of the polynomial remainders.

Basu, Pollack, and Roy [7] employ the so called *signed* `prem` function defined by

$$\mathrm{LC}(g)^{\delta} \cdot f = q \cdot g + h, \tag{3}$$

whereby, if $\mathrm{mod}(\delta, 2) = 1$ they set it to $\delta = \delta + 1$. This way they are able to exactly compute the signs of prs's (b) and (d), which are, therefore, called *signed* prs's. The signs of the other two prs's, (a) and (c), *may* not be exactly computed, and are, hence, called *non-signed* prs's.

Instead, we employ the so called `rem_z` pseudo-remainder function defined by

$$|\,\mathrm{LC}(g)|^{\delta} \cdot f = q \cdot g + h \tag{4}$$

and are able to exactly compute the signs of *all four* prs's. Moreover, we have shown that these four prs's are related as shown in Figure 1.

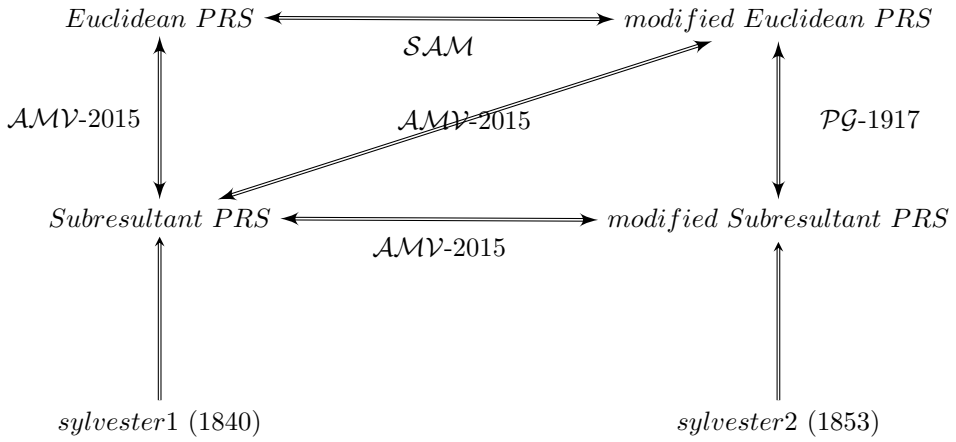


Figure 1: The double ended arrows indicate one-to-one correspondences that exist between the coefficients of the polynomials in the respective nodes. The labels indicate those who first established the correspondences and when. Two different matrices by Sylvester are used [16], [17].

In our work [1] – [6] — which relies heavily on the work by Pell and Gordon [15] — we have shown that *all four prs's* are *signed*, i.e. their signs are *uniquely* defined. To wit, the signs of the prs's computed in $\mathbb{Z}[x]$ are identical to those computed in $\mathbb{Q}[x]$.

Moreover, we have developed the `sympy/sage` module `subresultants_qq_zz.py`[1] for exactly computing the signs of all four prs's of Figure 1, employing the so called `rem_z` pseudo-remainder function defined in (4).

Our talk will focus on the functions included in this module — filling thus a vacuum in the educational process. Namely, when people teach about prs's in general — and subresultant prs's in particular — they would have a module to work with in order to compute the sequences with their correct signs. Otherwise they would have to say that they compute the sequences "up to sign" ([13], p. 182) & ([14], Example 4.7).

[1] `https://github.com/sympy/sympy/blob/master/sympy/polys/subresultants_qq_zz.py`.

References

[1] Akritas, A. G. A Simple Proof of the Validity of the Reduced PRS Algorithm. *Computing*, **38**, (1987), 369–372.

[2] Akritas, A. G., G. I. Malaschonok, P. S. Vigklas On a Theorem by Van Vleck Regarding Sturm Sequences. *Serdica Journal of Computing*, **7**(4), 101–134, 2013.

[3] Akritas, A. G., G. I. Malaschonok, P. S. Vigklas Sturm Sequences and Modified Subresultant Polynomial Remainder Sequences. *Serdica Journal of Computing*, **8**(1), 29–46, 2014.

[4] Akritas, A. G. Three New Methods for Computing Subresultant Polynomial Remainder Sequences (PRS's). *Serdica Journal of Computing*, *Serdica Journal of Computing*, **9**(1) (2015), 1–26.

[5] Akritas, A. G., G. I. Malaschonok, P. S. Vigklas On the Remainders Obtained in Finding the Greatest Common Divisor of Two Polynomials. *Serdica Journal of Computing*, **9**(2) (2015), 123–138.

[6] Akritas, A. G., G. I. Malaschonok, P. S. Vigklas A Basic Result on the Theory of Subresultants. *Serdica Journal of Computing*, to appear.

[7] Basu, S., R. Pollack, M. F. Roy *Algorithms in Real Algebraic Geometry*, 2nd Edition, Springer, 2006.

[8] Brown, W. S. The subresultant PRS Algorithm. *ACM Transactions on Mathematical Software*, **4**(3), (1978), 237–249.

[9] Brown, W. S., J. F. Traub On Euclid's Algorithm and the Theory of Subresultants. *Journal of the Association for Computing Machinery*, **18**, (1971), 505–514.

[10] Cohen, J. E. *Computer Algebra and Symbolic Computation – Mathematical Methods*. A.K. Peters, Massachusetts, (2003).

[11] Collins, G. E. Polynomial Remainder Sequences and Determinants. *American Mathematical Monthly*, **73**(7), (1966), 708–712.

[12] Collins, G. E. Subresultants and Reduced Polynomial Remainder Sequences. *Journal of the Association for Computing Machinery*, **14**, (1967), 128–142.

[13] von zur Gathen, J., J. Gerhard *Modern Computer Algebra*. Cambridge University Press, (1999).

[14] von zur Gathen, J., T. Lücking Subresultants Revisited. *Theoretical Computer Science*, **297**(1-3), (2003), 199–239.

[15] Pell, A. J., R. L. Gordon The Modified Remainders Obtained in Finding the Highest Common Factor of Two Polynomials. *Annals of Mathematics*, Second Series, **18**(4), (Jun., 1917), 188–193.

[16] Sylvester, J. J. A method of determining by mere inspection the derivatives from two equations of any degree. Philosophical Magazine, **16**, (1840), 132–135.

[17] Sylvester, J. J. On the Theory of Syzygetic Relations of Two Rational Integral Functions, Comprising an Application to the Theory of Sturm's Functions, and that of the Greatest Algebraical Common Measure. *Philosophical Transactions*, **143**, (1853), 407–548.

Automated Function Analysis for Calculus

A. Naiman[1]

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

When teaching basic mathematics courses, at all levels, there are *many* opportunities to include CAS packages like *Mathematica* [2], Maple [1], REDUCE [3], Sage [4], amongst many others. Computer algebra packages assist with the preparation of:

- classroom slides/notes,
- individualized homework assignments,
- in-class, randomized quizzes,
- class projects,
- extra-credit, further reading,
- final examinations,
- etc.

In this paper we discuss only the first area, i.e., that of the preparation of lecture notes, and particularly, for the teaching of basic, first-semester calculus.

About midway through the semester, one teaches the analysis of various functions: domains, ranges, symmetries, periodicity, monotonicity, extreme values, zeros, (one-sided) continuity, (one-sided) derivatives, etc. Furthermore, one needs to properly plot these functions for the added visual effect. As the analysis paves the way for very basic understanding of functions, we present many examples of these analyses during our lectures.

We have set about achieving effective, pedagogic, step-by-step methods for teaching this material. In order to convey the recipe for these analyses, we have also delved into *Mathematica* to find the most relevant functions. These in turn have myriads of options, and those we present as well, in order to best take advantage of the functions and their pedagogic capabilities. Finally, we include some of the pitfalls (learned the hard way!) of this approach, and how to circumvent them.

The most important aspect of the work, is that the process is *automated*, to be able to handle most/all of the basic types of functions learned during this part of Calculus I. We will present many examples of what does, and does not work, for these analyses, in the *Mathematica* environment.

References

[1] *Maple* at http://www.maplesoft.com/products/Maple/
[2] *Mathematica* at http://www.wolfram.com/mathematica/
[3] *REDUCE* at http://reduce-algebra.com/
[4] *Sage* at http://www.sagemath.org/

DUDAMATH The Digital Environment For Demonstrating Mathematical Ideas and Problem Solving

Ethan Hall, Dudamath.com., Israel
Leo Zak, Levinsky College of Education, Israel
Shirley Gitelman, Levinsky College of Education, Israel
Anatoli Kouropatov, Levinsky College of Education, Israel

Abstract

DUDAMATH is a digital environment for demonstrating mathematical ideas and problem solving. This environment grew from tools that were developed by the first presenter of this talk for school classes in order to provide a solution for needs that existing tools could not address. The main components of this environment are interactive arithmetic and algebraic expressions that can be manipulated in dynamic and diverse ways. These manipulations can then be documented and saved. Other highlights of the environment are diversity of representations, integrality that stresses the relation and connection between different subjects and aspects, and convenience of use and implementation in classrooms.

The use of technology can offer a lot to school math education. The interactivity and dynamics that technology can supply allow the creation of "virtual manipulatives": virtual objects that allow teachers to present and demonstrate mathematical principles. It allows students to explore these objects and reach conclusions about their properties and relations between them by considering the effect of the manipulations performed on them [1].

The symbolic expressions in DUDAMATH are interactive virtual manipulatives. Dynamic manipulations of these expressions are done by dragging or clicking them. Students can learn about the properties and behaviors of these expressions by trial and error, similar to how we learn about our physical environment. Students can observe dynamically how manipulations occur from stage to stage, and go back to cancel previous manipulations, lessening the common fear that results from making mistakes on paper. The way expressions react to manipulations is designed using the hierarchical structure of the expressions, in a way that is meant to strengthen the understanding of the relation between the structure of the expressions and the manipulations that were performed on them.

In the conference we will demonstrate the environment, an example of practical use, and will discuss its possible implications on mathematics education in school.

References

[1] Moyer-Packenham, P.S., & Westenskow, A. (2013) Effects of virtual manipulatives on student achievement and mathematics learning. *International Journal of Virtual and Personal Learning Environments (IJVPLE)*, 4(3), 35-50.

[2] Arcavi, A. (2003) The role of visual representations in the learning of mathematics. *Educational studies in mathematic*, 52(3), 215-241.

The use of digital tools to confront errors

Regina Ovodenko and Anatoli Kouropatov

Center for Educational Technology, Israel

The math education community places much importance on information regarding the conceptualization of learners of different mathematical subjects and regarding typical errors in these subjects. This type of information is essential for teachers for teaching planning and practice ([8], [11],[7], [9]). The question that has engaged math educators for many years is how we can confront these errors (see [2], [3],[4]).

In recent years, technological tools were developed in order to support the teaching practice. These tools are supposed to help in confronting typical errors, especially those related to concepts that possess a strong visual character, such as the inflection point. Informed use of these tools presents an interesting and actual didactic challenge (see [6]).

In the spirit of this tendency, the Center for Educational Technology developed a digital environment for learning and teaching mathematics for 10th, 11th, and 12th grades in high school - Challenge 5. The development of this environment was informed by research about the use of technological tools in math education and research about typical errors in specific mathematical subjects, such as the function (Carlson, 1998), tangent ([1], [10], [13]), inflection point ([12]), and similar.

This environment is made up of teaching units that include PowerPoint presentations, geogebra labs, interactive digital questionnaires, and videos. The use of these units allows teachers to plan lessons enriched by technology that, among other things, should prevent the typical errors .

In the conference we will present typical errors related to the concept of the inflection point (see [12]) and we will show ways of confronting these errors using digital tools. We will demonstrate how a specific digital tool can be used to design a teaching unit that allows teachers to address errors. The teaching unit includes the tool itself, the investigative assignment based on it, and a variety of other assignments. In addition, we will discuss how this approach of using a digital tool to create a teaching unit can be useful for confronting errors related to other concepts.

References

[1] M. Artigue. *The importance and limits of epistemological work in didactics*. In W. Geeslin and K. Graham (Eds.), Proceedings of the 16th Conference of the International Group for the

Psychology of Mathematics Education Vol.3, pp.195-216. Durham, NH: University of New Hampshire: PME (1992).

[2] R. Borasi. *Using errors as springboards for the learning of mathematics*, Focus on Learning Problems in Mathematics, 7(3-4), 1-14 (1985).

[3] R. Borasi. *Exploring mathematics through the analysis of errors*, For the Learning of Mathematics, 7, 1-8 (1987).

[4] R. Borasi. *Capitalizing on errors as "springboards for inquiry": A teaching experiment*, Journal for Research in Mathematics Education, 25, 166-208 (1994).

[5] Challenge 5: $http://lo.cet.ac.il/player/?document=d6beaef0-48a8-4250-b42d-c98cfae422a6\&language=he$. CET: Israel. (2016).

[6] P. Drijvers, M. Doorman, P. Boon, H. Reed and K. Gravemeijer. *The teacher and the tool: Instrumental orchestrations in the technology-rich mathematics classroom*, Educational Studies in Mathematics, 75, 213-234 (2010).

[7] National Council of Teachers of Mathematics. *Principles and Standards for School Mathematics*. Reston, Virginia: NCTM (2000)

[8] P. Samovol, and M. Applebaum. *Find the mistake*, Journal for Mathematics Teachers, 30, 45-48 (2003). (In Hebrew).

[9] L.S. Shulman. *Those who understand: Knowledge growth in teaching*, Educational Researcher, 15, 4-14 (1986).

[10] D. Tall. *Constructing the concept image of a tangent*, In J. Bergeron, N. Herscovics and C. Kieran (Eds.), Proceedings of the 11th Conference of the International Group for the Psychology of Mathematics Education (Vol. 3, pp. 69-75). Montreal, Canada: PME (1987).

[11] P. Tsamir and R. Barkai. *The use of errors in teaching mathematics: theory and practice*, Tel Aviv: Ramot (2005). (In Hebrew).

[12] P. Tsamir and R. Ovodenko. *University students' grasp of inflection points*, Educational Studies in Mathematics 83, 409-427 (2013).

[13] S. Vinner. *Conflicts between definitions and intuitions - the case of the tangent*, in A. Vermandel (Ed.), Proceedings of the 6^{th} International Conference for the Psychology of Mathematical Education, pp. 24-29, Antwerp, Belgium: PME (1982).

Computer-Algebra-Aided Chebyshev Methods for Ordinary Differential Equations

M. Xue[1]

[1] *Vroom Laboratory for Advanced Computing, USA, mxue@vroomlab.com*

The solution of ordinary differential equation can be approximated by a linear combination of so called basis functions. Using the Chebyshev Polynomials as the basis functions, the approximation can be expressed as

$$y(x) = \sum_{r=0}^{\infty} a_r T_r(x) \tag{1}$$

where $T_r(x)$'s are Chebyshev Polynomials of degree r, and a_r's are the coefficients to be determined. In practice, we seek the approximation using a truncated expression of (1), namely,

$$\sum_{r=0}^{n} a_r T_r(x) \tag{2}$$

An online Computer Algebra System (CAS) is used to generate and subsequently solve a system of equations concerning a finite number of a_r's. The use of CAS allows the retention of more a_r's in (2). It also obviates the need for the traditional pad and pencil computations.

Examples will be given to illustrate this approach in solving initial value problems, boundary value problems as well as eigenvalue problems for ordinary differential equations whose coefficients and other terms are themselves polynomials.

References

[1] L. Fox and D.F. Mayers, *Numerical Solution of Ordinary Differential Equations*, pp. 179-197 (1987).

[2] G.H. Golub and J.M. Ortega, *Scientific Computing and Differential Equations*, pp. 179-185 (1992).

[3] *Omega: A Computer Algebra System Explorer*, at http://www.omega-math.com

Teaching complex potential model to students of environmental engineering faculty 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

In this talk we would like to present some our experiences with teaching elements of complex analysis to students of Environmental Engineering Faculty of Warsaw University of Life Science. Complex analysis in this faculty was one of the parts of higher mathematics course. In the framework of this course complex potential fluid flow model in two dimensions was presented. Complex potential is defined as a holomorphic function of a complex variable $f(z) = f(x+iy) = g(x,y) + ih(x,y)$. To understand this model and to be able to solve connected with it tasks, the ability to calculate complex derivatives and integrals along a curve is required. Using CAS programs for teaching the model it seems to be very useful to simplify complex expressions, calculate complex derivatives and integrals and also to present trajectories of the fluid particles graphically and dynamic plot of particle motion. In the framework of our talk we would like to present several examples solving of typical tasks from complex potential for our students using Mathematica. They include determination of complex velocity and circulation of velocity field along a closed curve, determination of the flux of a fluid across the curve and drawing trajectories of the fluid particles. We will also present particles motion animation along the trajectories.

References

[1] K. Sato, *Complex analysis for practical engineering*, Springer, 2015
[2] M. Spiegel, *Schaum's Outline of Complex Variables.* McGraw-Hill, 1981
[3] Y. K. Kwok, *Applied Complex Variables for Scientists and Engineers.* Cambridge University Press, 2002
[4] H. Ruskeepaa *Mathematica Navigator: Graphics and Methods of applied Mathematics.* Academic Press, Boston (2005)
[5] S. Wolfram *The Mathematica Book.* Wolfram Media/ Cambridge University Press (1996)

Session 2

Applied and Computational Algebraic Topology

Session chairs:

Graham Ellis
School of Mathematics, National University of Ireland, Galway, Ireland

Marian Mrozek
Institute of Computer Science and Computational Mathematics, Jagiellonian University, Poland

Aniceto Murillo
Departamento de Algebra, Geometria y Topologia, Universidad de Malaga, Spain

Pedro Real
Institute of Mathematics (IMUS), University of Seville, Spain

Eduardo Saenz de Cabezon
Mathematics and Computation, Universidad de La Rioja, La Rioja, Spain

Solving Systems of Equations with Uncertainty

P. Franek, M. Krčál, H. Wagner

[1] *IST Austria peter.franek@ist.ac.at*
[2] *IST Austria marek.krcal@gmail.com*
[3] *IST Austria, hwagner@ist.ac.at*

We study the problem of detecting zeros of continuous functions $\mathbb{R}^n$-valued functions that are known only up to an error bound, extending the earlier theoretical work [1] with explicit algorithms and experiments with an implementation [2].

The domain X of f is a simplicial complex and our partial knowledge of f is based on approximate function values in vertices. The algorithm first identifies a subdomain A where the function f is provably non-zero, a simplicial approximation $f' : A \to S^{n-1}$ of $f/|f|$, and then verifies *non-extendability* of f' to a map $X \to S^{n-1}$ to certify a zero. Deciding extendability is based on computing the cohomological *obstructions* and their persistence. We describe an explicit algorithm for the *primary and secondary obstruction*, two stages of a sequence of algorithms with increasing complexity. Using elements and techniques of persistent homology, we quantify the persistence of these obstructions and hence of the robustness of zero.

We provide experimental evidence that for random Gaussian fields, the *primary obstruction*—a much less computationally demanding test than the secondary obstruction—is typically sufficient for approximating robustness of zero. Further, we offer a possible geometric explanation of this observed phenomenon.

References

[1] Franek, P. and Krčál, M., *Robust Satisfiability of Systems of Equations*, J.ACM 2015, 62, 26:1–19.

[2] Franek, P. and Krčál, M. and Wagner, H. *Solving equations and optimisation problems with uncertainty*, preprint arXiv:1607.06344

Computing simplicial representatives of homotopy group elements

Marek Filakovský [1], Peter Franek [2] , Uli Wagner [3] , Stephan Zhechev [4]

[1] *IST AUSTRIA , marek.filakovsky@ist.ac.at*

[2] *IST AUSTRIA , peter.franek@ist.ac.at*

[3] *IST AUSTRIA , uli@ist.ac.at*

[4] *IST AUSTRIA , stephan.zhechev@ist.ac.at*

A central problem of algebraic topology is to understand the *homotopy groups* $\pi_d(X)$ of a topological space X. For the computational version of the problem, it is well known that there is no algorithm to decide whether the *fundamental group* $\pi_1(X)$ of a given finite simplicial complex X is trivial. On the other hand, there are several algorithms that, given a finite simplicial complex X that is *simply connected* (i.e., with $\pi_1(X)$ trivial), compute the higher homotopy group $\pi_d(X)$ for any given $d \geq 2$.

However, these algorithms come with a caveat: They compute the isomorphism type of $\pi_d(X)$, $d \geq 2$ as an *abstract* finitely generated abelian group given by generators and relations, but they work with very implicit representations of the elements of $\pi_d(X)$. Converting elements of this abstract group into explicit geometric maps from the d-dimensional sphere S^d to X has been one of the main unsolved problems in the emerging field of computational homotopy theory.

Here we present an algorithm that, given a simply connected simplicial complex X, computes $\pi_d(X)$ and represents its elements as simplicial maps from a suitable triangulation of the d-sphere S^d to X. For fixed d, the algorithm runs in time exponential in size(X), the number of simplices of X. Moreover, we prove that this is optimal: For every fixed $d \geq 2$, we construct a family of simply connected simplicial complexes X such that for any simplicial map representing a generator of $\pi_d(X)$, the size of the triangulation of S^d on which the map is defined is exponential in size(X).

References

[1] S. I. Adyan. Algorithmic unsolvability of problems of recognition of certain properties of groups. *Dokl. Akad. Nauk SSSR (N.S.)*, 103:533–535, 1955.

[2] D. J. Anick. The computation of rational homotopy groups is $\#\wp$-hard. Computers in geometry and topology, Proc. Conf., Chicago/Ill. 1986, Lect. Notes Pure Appl. Math. 114, 1–56, 1989.

[3] C. Berger. *An effective version of the Hurewicz theorem.* Theses, Université Joseph-Fourier - Grenoble I, 1991. URL: `https://tel.archives-ouvertes.fr/tel-00339314`.

[4] Clemens Berger. Un groupoïde simplicial comme modèle de l'espace des chemins. *Bulletin de la Societé mathematique de France*, 123(1):1–32, 1995.

[5] E. H. Brown (jr.). Finite computability of Postnikov complexes. *Ann. Math. (2)*, 65:1–20, 1957.

[6] M. Cadek, M. Krcál, J. Matoušek, Lukás Vokřínek, and Uli Wagner. Extending continuous maps: polynomiality and undecidability. In *STOC*, pages 595–604, 2013.

[7] M. Čadek, M. Krčál, J. Matoušek, F. Sergeraert, L. Vokřínek, and U. Wagner. Computing all maps into a sphere. *J. ACM*, 61(3):17:1–17:44, June 2014.

[8] M. Čadek, M. Krčál, J. Matoušek, L. Vokřínek, and U. Wagner. Extendability of continuous maps is undecidable. *Discr. Comput. Geom.*, 51(1):24–66, 2013.

[9] M. Čadek, M. Krčál, J. Matoušek, L. Vokřínek, and U. Wagner. Polynomial-time computation of homotopy groups and Postnikov systems in fixed dimension. *Siam Journal on Computing*, 43(5):1728–1780, 2014.

[10] Martin Čadek, Marek Krčál, and Lukáš Vokřínek. Algorithmic solvability of the lifting-extension problem. *Discrete & Computational Geometry*, pages 1–51, 2017.

[11] H. Edelsbrunner and J. Harer. *Computational Topology: An Introduction*. Applied mathematics. American Mathematical Society, 2010. URL: `https://books.google.cz/books?id=MDXa6gFRZuIC`.

[12] Herbert Edelsbrunner and Daniel R. Grayson. Edgewise subdivision of a simplex. In *Proceedings of the Fifteenth Annual Symposium on Computational Geometry*, SCG '99, pages 24–30, New York, NY, USA, 1999. ACM.

[13] Steve Ferry and Shmuel Weinberger. Quantitative algebraic topology and lipschitz homotopy. *Proceedings of the National Academy of Sciences*, 110(48):19246–19250, 2013.

[14] M. Filakovský. Effective chain complexes for twisted products. Preprint, 2012. URL: `arXiv:1209.1240`.

[15] M. Filakovský and L. Vokřínek. Are two given maps homotopic? An algorithmic viewpoint. *ArXiv e-prints*, 2013. `arxiv.org/abs/1312.2337` `arXiv:1312.2337`.

[16] P. Franek and M. Krčál. Robust satisfiability of systems of equations. *J. ACM*, 62(4):26:1–26:19, 2015.

[17] Michael Freedman and Vyacheslav Krushkal. Geometric complexity of embeddings in R^d. Geometric and Functional Analysis, 24(5):1406–1430, 2014.

[18] P. G. Goerss and J. F. Jardine. *Simplicial homotopy theory*. Birkhäuser, Basel, 1999.

[19] M. Gromov. Quantitative homotopy theory. *Prospects in Mathematics: Invited Talks on the Occasion of the 250th Anniversary of Princeton University (H. Rossi, ed.)*, pages 45–49, 1999.

[20] A. Haefliger. Plongements différentiables dans le domaine stable. *Comment. Math. Helv.*, 37:155–176, 1962/1963.

[21] A. Hatcher. *Algebraic Topology*. Cambridge University Press, Cambridge, 2001.

[22] J. Heras, V. Pascual, J. Rubio, and F. Sergeraert. fKenzo: a user interface for computations in algebraic topology. *J. Symb. Comput.*, 46(6):685–698, 2011.

[23] D. Kan. The Hurewicz Theorem. In *International Symposium of Algebraic Topology, Autonomous University of Mexico and UNESCO*, pages 225–231, 1958.

[24] D. M. Kan. A combinatorial definition of homotopy groups. *Annals of Mathematics*, 67(2):282–312, 1958.

[25] R. Kannan and A. Bachem. Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix. *SIAM J. Computing*, 8:499–507, 1981.

[26] S. O. Kochman. *Stable homotopy groups of spheres. A computer-assisted approach.* Lecture Notes in Mathematics 1423. Springer-Verlag, Berlin etc., 1990.

[27] M. Krčál, J. Matoušek, and F. Sergeraert. Polynomial-time homology for simplicial Eilenberg–MacLane spaces. *Foundat. of Comput. Mathematics*, 13:935–963, 2013.

[28] Isaac Mabillard and Uli Wagner. Eliminating higher-multiplicity intersections, II. The deleted product criterion in the r-metastable range. In *Proc. 32nd International Symposium on Computational Geometry (SoCG 2016)*, pages 51:1–51:12, 2016.

[29] J. Matoušek, M. Tancer, and U. Wagner. Hardness of embedding simplicial complexes in R^d. *J. Eur. Math. Soc.*, 13(2):259–295, 2011.

[30] J. Matoušek. Computing higher homotopy groups is $W[1]$-hard. *Fundamenta Informaticae*, 2014.

[31] Jiří Matoušek, Eric Sedgwick, Martin Tancer, and Uli Wagner. Embeddability in the 3-sphere is decidable. In *Proceedings of the Thirtieth Annual ACM Symposium on Computational Geometry*, SOCG'14, pages 78–84, New York, NY, USA, 2014.

[32] S. Matveev. *Algorithmic Topology and Classification of 3-Manifolds*. Springer, 2007.

[33] J. P. May. *Simplicial Objects in Algebraic Topology*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 1992. Reprint of the 1967 original.

[34] J. R. Munkres. *Elements of Algebraic Topology*. Addison-Wesley, Reading, MA, 1984.

[35] D.G. Quillen. *Homotopical Algebra*. Lecture Notes in Mathematics. Springer Berlin Heidelberg, 1967.

[36] M. O. Rabin. Recursive unsolvability of group theoretic problems. *Ann. of Math. (2)*, 67:172–194, 1958.

[37] D. C. Ravenel. *Complex Cobordism and Stable Homotopy Groups of Spheres (2nd ed.)*. Amer. Math. Soc., 2004.

[38] P. Real. An algorithm computing homotopy groups. *Mathematics and Computers in Simulation*, 42:461—465, 1996.

[39] A. Romero, J. Rubio, and F. Sergeraert. Computing spectral sequences. *J. Symb. Comput.*, 41(10):1059–1079, 2006.

[40] A. Romero and F. Sergeraert. Effective homotopy of fibrations. *Applicable Algebra in Engineering, Communication and Computing*, 23(1-2):85–100, 2012.

[41] A. Romero and F. Sergeraert. A Bousfield–Kan algorithm for computing the effective homotopy of a space. *Foundations of Computational Mathematics*, pages 1–32, 2016.

[42] J. Rubio and F. Sergeraert. Constructive algebraic topology. *Bull. Sci. Math.*, 126(5):389–412, 2002.

[43] J. Rubio and F. Sergeraert. Algebraic models for homotopy types. *Homology, Homotopy and Applications*, 17:139–160, 2005.

[44] J. Rubio and F. Sergeraert. Constructive homological algebra and applications. Preprint, `arXiv:1208.3816`, 2012.

[45] R. Schön. *Effective Algebraic Topology*. Memoirs of the American Mathematical Society. American Mathematical Society, 1991.

[46] F. Sergeraert. The computability problem in algebraic topology. *Adv. Math.*, 104(1):1–29, 1994.

[47] J. R. Smith. m-Structures determine integral homotopy type. Preprint, `arXiv:math/9809151v1`, 1998.

[48] R. I. Soare. Computability theory and differential geometry. *Bull. Symbolic Logic*, 10(4):457–486, 2004.

[49] L. Vokřínek. Decidability of the extension problem for maps into odd-dimensional spheres. *Discrete & Computational Geometry*, 57(1):1–11, 2017.

[50] C. Weber. Plongements de polyèdres dans le domaine metastable. *Comment. Math. Helv.*, 42:1–27, 1967.

[51] A. J. Zomorodian. *Topology for Computing*, volume 16 of *Cambridge Monographs on Applied and Computational Mathematics*. Cambridge University Press, Cambridge, 2005.

Comparison and parallelization possibilities of algebraic topology-based verification tools for equations systems

Bartłomiej Jacek Kubica[1]

[1] *Department of Applied Informatics, Warsaw University of Life Sciences, Poland, bartlomiej_kubica@sggw.pl*

Let us consider solving the nonlinear system of equations:

$$f\colon X \to \mathbb{R}^m, \text{ where } X \subseteq \mathbb{R}^n \text{ and } n \geq m\ . \tag{1}$$

Interval methods (see, e.g., [8]) have proven to be useful, in particular, in solving such systems. One of their advantages is allowing not only to locate solutions of well-determined and underdetermined systems, but also to *verify* them, i.e., prove that in a given box there is a solution point (resp. a segment of the solution manifold).

The most celebrated tool allowing such verification is the interval Newton operator (cf., e.g., [8]). Despite its advantages, it is not the only existence verification test. Other ones, based, i.a., on the theorem of Miranda [8] are used as well.

Particularly interesting is a class of existence verification tools based on the algebraic topology notions. They can, for instance, use Borsuk theorem [5], compute the topological degree [3, 4] or use the obstruction theory and other advanced tools and notions [2].

This paper has three goals: to make a short survey of such techniques, to consider their parallel implementation and propose a new potential technique. As interval algorithms usually are instances of the branch-and-prune (B&P) or other subdivision-based schemes, their parallelization is often based of concurrent processing of different boxes and not on parallelizing the investigation of a single box. Nevertheless, as discussed, i.a., in [11], parallel processing of a single box is also important and its importance is likely to increase in the future.

The framework we use for implementing and investigating all tools is HIBA_USNE [7], described in a series of papers of the first author (see [9, 10, 11] and the references therein).

Borsuk test. This is one of the tests, dealing – in its original form – with well-determined problems. It is based on one of theorems of Karol Borsuk

states (slightly simplifying) that the function $f(\cdot)$ must have a zero on the box $\boldsymbol{x}$, if:

$$f(\operatorname{mid}\boldsymbol{x} + r) \neq \lambda \cdot f(\operatorname{mid}\boldsymbol{x} - r),\ \forall \lambda > 0 \text{ and } \operatorname{mid}\boldsymbol{x} + r \in \partial\boldsymbol{x}\ . \qquad (2)$$

The test has to compute the intersection of several interval expressions to prove that there is no λ for which the disequality (2) becomes an equality.

Such an intersection can be computed in parallel, e.g., using the reduction operation.

Topological degree test. This is another approach to prove existence of the solution for well-determined problems.

Computing the topological degree of a function over a box, suggested in several papers, is very useful to prove the existence of the solution; even though it requires relatively high computational effort. The algorithm proposed in [3] is recursive; hence, it can be parallelized in a relatively easy manner. There are several interesting details about this approach and the paper is going to describe and discuss some of them, in particular data structures used to store adjacent subboxes in the subdivision of the boundary.

How to deal with underdetermined problems? In [9], the author described how the interval Newton operator can be used to verify an underdetermined system of equations. Succinctly, if we have m equations in $n > m$ variables, we need to choose a square submatrix of the Jacobi matrix. Treating the chosen m variables normally and the remaining $(n - m)$ ones as parameters, we can perform an normal Newton iteration to to narrow, discard or verify the existence of solution *for all* values of the $(n - m)$ "parameters".

It can simply be proven that a similar procedure can be performed for the Borsuk test and topological degree test. It is an open (and interesting) problem, how to choose the m (out of n) variables for the verification. [9] proposes a policy, but there is place for further improvements, certainly.

In any case, due to the nature of interval calculus, such an approach can verify boxes where the solution exists *for all* values of the other $(n - m)$ variables. For instance, when we verify a single equation in two variables, such methods can verify a solution segment on the left in Fig. 1, but not the one on the right. Actually, for a single equation $f(x) = 0$, we could find two points x_a and x_b such that $f(x_a) \cdot f(x_b) < 0$, which would prove that any connected line containing these points contains a solution. This is a direct consequence of the intermediate value theorem. Unfortunately, the theorem does not extend simply to more equations.

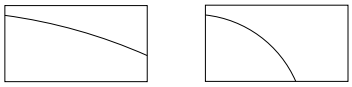


Figure 1: Left: a solution segment relatively easy to verify using interval tests, right: the hard one

Obstruction theory test. In a series of papers (see, e.g., [2, 3] or references therein), Franek et alii propose a fascinating family of methods targeted specifically at underdetermined systems. To be succinct, the methods try to approximate the "suspicious" box as a cell complex or a simplicial set and they construct a Postnikov complex, build of Eilenberg-MacLane spaces. Basing on this representation, we can check possible extendability of a function for subsequent skeletons of the complex.

This test seems a pretty general tool, suitable for underdetermined problems as well as well-determined ones (in the latter case it is equivalent to using the topological degree). Unfortunately, it is also cumbersome to implement and usually requiring high computational effort. Eilenberg-MacLane spaces have often infinite dimensionality and thus they can only be represented implicitly.

Also, please note that existing software such as GUDHI [6] is of little help when implementing this test and some of the useful algorithms might even occur to be unimplementable, like, e.g., the Brown's algorithm [1].

Ironically, though the algorithm is hard to implement, its parallelization should be natural; operations on various simplices (or cells) of the complex can be performed concurrently.

A new test for two equations. This test is an original idea of the author. The test is limited to the case $m = 2$, $n \geq 2$, but it is implementable using existing software and might be useful in some practical cases. Actually, the toolset is pretty similar to the one used by Franek et alii [3], but these tools get arranged in a quite new manner.

Assume we have found in the function's domain, a cubical complex C that is homotopically equivalent to a one-dimensional circle S^1(other words: a closed path in the boundary). Assume the image of C is homotopically equivalent to $S^1 \subset \mathbb{R}^2$, also; other words: it does not contain $(0, 0)$ and it winds around this point (its winding number aka topological degree is different from zero). We should be able to find such C, by performing a graph-like algorithm on the cubical complex representing the boundary of the considered box (seeking for cycles) and checking the sign vector of adjacent

boxes. Please note that segments of C can belong to arbitrary faces of the considered box, e.g., Fig. 2.

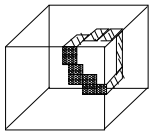


Figure 2: Representation of C

It can be proven that (under proper technical assumptions) for any k-dimensional sphere S^k such that $C \subseteq S^k \subseteq X$, S^k contains a zero of f.

This theorem can probably be generalized to $m > 2$, but it might not be efficient for higher dimensions. Details remain to be determined.

References

[1] E. H. Brown, *Finite computability of Postnikov complexes*, Annals of Mathematics, **1957**, pp. 1–20 (1957).

[2] P. Franek and M. Krčál, *Robust satisfiability of systems of equations*, in *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms*, SIAM, pp. 193–203 (2014).

[3] P. Franek and S. Ratschan, *Effective topological degree computation based on interval arithmetic*, Mathematics of Computation. **84**, 293, pp. 1265–1290 (2015).

[4] A. Frommer and F. Hoxha and B. Lang, *Proving the existence of zeros using the topological degree and interval arithmetic*, Journal of Computational and Applied Mathematics, **199**, 2, pp. 397–402 (2007).

[5] A. Frommer and B. Lang, *On preconditioners for the Borsuk existence test*, PAMM, **4**, 1, pp.638-639 (2004).

[6] *GUDHI* C++ library, `http://gudhi.gforge.inria.fr/` (2017).

[7] *HIBA_USNE*, C++ library, `https://www.researchgate.net/publication/316687827_HIBA_USNE_Heuristical_Interval_Branch-and-prune_Algorithm_for_Underdetermined_and_well-determined_Systems_of_Nonlinear_Equations_-_Beta_25` (2017).

[8] R. B. Kearfott, *Rigorous Global Search: Continuous Problems*, Kluwer, Dordrecht, 1996.

[9] B. J. Kubica, *Interval methods for solving underdetermined nonlinear equations systems*, Reliable Computing, **15**, pp.207–217 (2011).

[10] B. J. Kubica, *Presentation of a highly tuned multithreaded interval solver for underdetermined and well-determined nonlinear systems*, Numerical Algorithms, **70**, 4, pp. 929–963 (2015).

[11] B. J. Kubica, *Parallelization of a bound-consistency enforcing procedure and its application in solving nonlinear systems*, Journal of Parallel and Distributed Computing, published online `https://doi.org/10.1016/j.jpdc.2017.03.009` (2017).

An attempt at using topology for classification.

N. Blaser[1], M. Brun[2]

[1] *University of Bergen, Norway, nello.blaser@uib.no*
[2] *University of Bergen, Norway, morten.brun@uib.no*

Objective: We aim to develop a classification algorithm based on topological concepts and to compare it to state of the art classification tools.

Status: Classification is a classical problem in statistics and machine learning concerned with the identification of classes of data. Typically there is some training data whose classes are known and the goal is to predict the classes of new data. Many standard algorithms for classification use the geometry of data as a basis for classification. These algorithms are often coordinate dependent.

The basic aim of topological data analysis is to study a finite point cloud P in a metric space M with topological methods, which by nature are coordinate independent. Topological features can be calculated by constructing a filtered topological space from P, and computing its persistent homology. These features have previously been used as a preprocessing step in classification [Adcock et al., 2016]. As far as we are aware the topological spaces used to calculate topological features have not previously been used directly for classification.

Devisive cover is an algorithm that has been developed to approximate persistent homology of the Čech filtration associated to P [Blaser and Brun, 2017]. From the point cloud P it produces a finite cover $\mathscr{U} = \{U_1, \ldots, U_n\}$ of M with the property that every element of the cover contains an element of P.

Methodology: The divisive cover algorithm consists of two components: a method to use a point cloud Q in M to produce a cover $\mathscr{U}^Q = \{U_0^Q, U_1^Q\}$ of M and a method to decide whether more divisions shall be performed and if so, which element of $\mathscr{U}$ to divide next.

Given these two methods the algorithm goes as follows: start with the cover $\mathscr{U}$ = $\{M\}$ of M. While more divisions should be performed, do the following:

1. Find the element U of $\mathscr{U}$ to divide next
2. For $Q = P \cap U$ replace the element U in $\mathscr{U}$ by the two elements $U \cap U_0^Q$ and $U \cap U_1^Q$ obtained from $\mathscr{U}^Q = \{U_0^Q, U_1^Q\}$.

As in [Blaser and Brun, 2017], our division method finds a pair (a_0, a_1) of extremal points in Q and uses these points to find the cover $\{U_0^Q, U_1^Q\}$. For $i = 0, 1$, the set U_i^Q consists of the points in M with distance to a_i less than or equal f times the distance to the other point a_{1-i} for some given factor $f = (1-\delta)/(1+\delta)$.

Given a set Y of classes of the elements of P and an element U of $\mathscr{U}$ we choose a dominant class for U, that is a class y containing the maximal number of points in $P \cap U$. The next element of $\mathscr{U}$ to divide is the element with the smallest proportion of points in the dominant class. We stop dividing when the average proportion of points in the dominant class in all elements of $\mathscr{U}$ is above a chosen misclassification treshold.

For a point $x \in M$ we consider the subset $\mathscr{U}_x \subseteq \mathscr{U}$ consisting of elements U of $\mathscr{U}$ containing x. To each class y we associate the number $\varphi(x, y, \mathscr{U})$ given as the sum over $U \in \mathscr{U}_x$ of the number of elements in $P \cap U$ of class y. We predict that the class of x is the class y maximizing $\varphi(x, y, \mathscr{U})$.

To illustrate how our method partitions the space M in classes we use two-dimensional data from [Hastie et al., 2009, Figure 2.1]. We compare classification accuracy of divisive cover, random forests [Breiman, 2001] and suport vector machines [Cortes and Vapnik, 1995] on datasets from the UCI Machine Learning Repository [Lichman, 2013]. For each dataset we first chose parameters for divisive cover. We then split the data in training and test data and compared the performance of the classification methods. Categorical data was converted to numeric data by creating a dummy variable for each category. We report the average accuracy of the methods for 100 random train-test splits.

Results Divisive cover classifications use topological features of a point cloud for classification. Figure 1 shows the decission boundaries for random forests, suport vector machines and divisive cover classification.

The classification accuracy of divisive cover classification was comparable with the classification accuracies of random forest and support vector machine. Table 1 shows a selection of classification results from different UCI datasets.

Significance of study: We present a new classification method based on topological ideas. This attempt at using topological methods for classification leads us to believe that topological methods can improve classification.

References

[Adcock et al., 2016] Adcock, A., Carlsson, E., and Carlsson, G. (2016). The ring of algebraic functions on persistence bar codes. *Homology Homotopy Appl.*, 18(1):381–402.

[Blaser and Brun, 2017] Blaser, N. and Brun, M. (2017). Filtered covers. *ArXiv e-prints*.

[Breiman, 2001] Breiman, L. (2001). Random forests. *Machine Learning*, 45(1):5–32.

[Cortes and Vapnik, 1995] Cortes, C. and Vapnik, V. (1995). Support-vector networks. *Machine Learning*, 20(3):273–297.

[Hastie et al., 2009] Hastie, T., Tibshirani, R., and Friedman, J. (2009). *The elements of statistical learning*. Springer Series in Statistics. Springer, New York, second edition. Data mining, inference, and prediction.

[Lichman, 2013] Lichman, M. (2013). UCI machine learning repository.

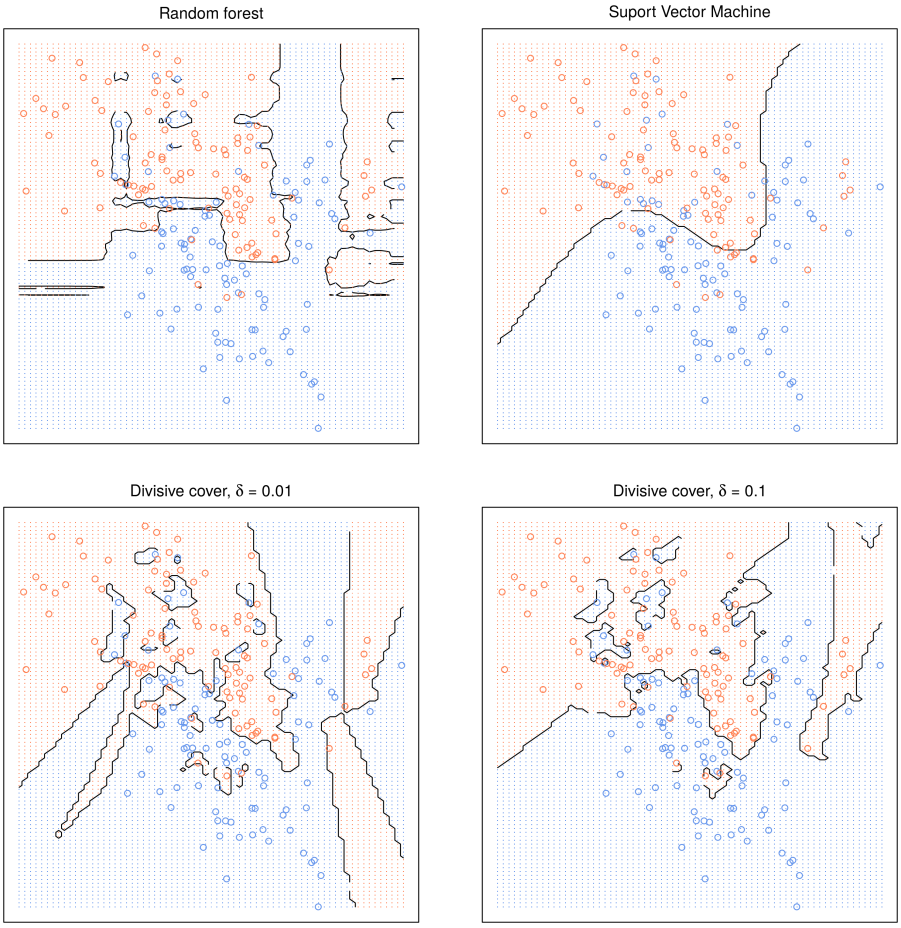


Figure 1: Classifications of sample data from [Hastie et al., 2009] by random forest, suport vector machine and divisive covers with $\delta = 0.01$ and $\delta = 0.1$.

data	method	metric	δ	treshold	% accuracy
anneal	random_forest	-	-	-	99.1
	divisive	hamming	0.01	0	96.7
	svm	-	-	-	95.3
	divisive	euclidean	0.001	0.0001	94.4
balance	svm	-	-	-	89.9
	random_forest	-	-	-	83.7
	divisive	euclidean	0.01	0.01	83.2
breast_w	random_forest	-	-	-	96.5
	divisive	euclidean	0.05	0.0	96.2
	svm	-	-	-	95.4
credit	random_forest	-	-	-	87.2
	divisive	hamming	0.05	0.01	83.8
	divisive	euclidean	0	0.05	67.5
	svm	-	-	-	56.6
diabetes	random_forest	-	-	-	75.6
	divisive	euclidean	0.05	0.01	71.4
	svm	-	-	-	64.8
digits	random_forest	-	-	-	97.3
	divisive	euclidean	0.01	0.0	89.6
	svm	-	-	-	39.0
glass	random_forest	-	-	-	75.7
	divisive	euclidean	0.07	0.0	68.9
	svm	-	-	-	61.4
hayes_roth	random_forest	-	-	-	80.8
	svm	-	-	-	76.6
	divisive	euclidean	0.02	0.05	70.4
hepatitis	random_forest	-	-	-	85.7
	svm	-	-	-	80.3
	divisive	hamming	0.0	0.1	80.0
	divisive	euclidean	0.005	0.15	78.8
iris	svm	-	-	-	97.2
	divisive	cosine	0.08	0.01	95.9
	random_forest	-	-	-	95.1
	divisive	euclidean	0.05	0.05	94.4

Table 1: Average classification accuracy comparing divisive cover with random forests and support vector machines on some standard datasets.

Towards a hole tree representation of 2D biomedical digital images

C. Alemán, F. Díaz-del-Río, P. Real

HTS Informatics Engineering, University of Seville, Spain {fdiaz, real}@us.es
This research is supported by the Spaniard (AEI/FEDER,UE) research project TOP4COG (Topological Recognition of 4D Digital Images via HSF model, MTM2016-81030-P).

Abstract

Due to the fact that the n-xel value of a digital biomedical image $I : D \to V$ has in general a physical meaning, both texture and shape interpretations are compulsory steps in biomedical image processing. The first attribute is commonly described in terms of notions like grain, regularity or homogeneity and quantified at pre-segmentation level by using texture metrics based on local intensity variations (statistical moments, co-ocurrence matrix measures, spectral measures, fractal dimensions, run-length statistics, Gabor filters,...). The second attribute is determined once the image has been previously segmented and it is measured in geometric terms like length, curvature or chain-code. We set out here a new topological tree-based representation of an original (non-segmented) 2D biomedical digital image which is contrast-invariant and from which it may be possible to generate informative many topological texture metrics, high-level segmentations and shape measures. This representation is based on the Homological Spanning Forest (HSF, for short) framework developed in [3, 4, 5]. From a HSF-model of a color digital image, it is possible to generate tree representations of the image based on clusters of 4-connected components, similarly to the method for building tree-of-shapes [1] or inclusion tree [2] models. Some potential descriptions of these hole tree representations are implemented and compared.
Keywords: 2D digital image, topological representation, tree-of-hole, Homological Spanning Forest

References

[1] Caselles, V., Meinhardt, E. and Monasse, P. Constructing the tree of shapes of an image by fusion of the trees of connected components of upper and lower level sets. *Positivity*, 12(1), 55–73, 2008.

[2] Monasse, P. and Guichard, F. (2000). G. E. Carlsson, G. Singh, and A. Zomorodian. Fast computation of a contrast-invariant image representation. *IEEE Transactions on Image Processing*, 9(5), 860-872, 2000.

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

[4] Molina-Abril, H. and Real, P. Homological spanning forest framework for 2D image analysis. *Annals of Mathematics and Artificial Intelligence*, 1-25, 2012

[5] Diaz-del-Rio, F., Real, P. and Onchis, D. M. A parallel homological spanning forest framework for 2D topological image analysis. *Pattern Recognition Letters*, 83, 49-58, 2016.

Monomial resolutions as a preprocessing for the computation of simplicial homology

A. Bigatti, J. Heras, E. Sáenz-de-Cabezón

[1] *Universitá degli Studi Genova, Italy*
[2] *Universidad de La Rioja, Spain*
[3] *Universidad de La Rioja, Spain*

The Stanley-Reisner correspondence [2] is one to one between square free monomial ideals and simplicial complexes. In this context, Hochster's formula shows that the Betti numbers of a square free monomial ideal are equivalent to the dimensions of the homology groups of its corresponding simplicial complex, cf. [1]. In particular we are interested in the Betti numbers of the ideal that occur at multi degree $x_1 \cdots x_n$ (i.e. the product of all variables). Usually, this correspondence is used to obtain resolutions and Betti numbers of monomial ideals via simplicial homology.

In this paper we explore the opposite direction, i.e. compute the dimensions of the homology groups of abstract simplicial complexes using monomial ideal resolutions. In particular we use the mapping cone resolution to either directly obtain the Betti numbers if possible or bounds for them. Using the Mayer-Vietoris tree algorithm [4] in a similar way as the authors did in [3] to compute $(n-1)$ Koszul homology of monomial ideals we obtain upper bounds for the dimensions of these groups and also the particular homological dimensions in which there can be nonzero homology discarding all the others, so that the usual simplicial homology computations would be reduced.

We propose the following algorithm:

-INPUT: an abstract simplicial complex Δ given by its facets

-OUTPUT: dimensions of its homology groups (a modifcation allows to obtain generators)

STEPS OF THE ALGORITHM:

1- Compute the Stanley-Reisner ideal I_Δ

2- Compute the MVTree of I_Δ obtaining $\beta_{i,\mu}(I_\Delta)$ or bounds

3- List the dimensions in which MVTree does not give the actual $\beta_{x_1,\ldots,x_n}(I_\Delta)$

4- In those dimensions apply the classical algorithm to obtain the dimensions of the homology groups of Δ.

References

[1] E. Miller and B. Sturmfels, Combinatorial Commutative Algebra, Springer 2004

[2] R. Stanley, Combinatorics and Commutative Algebra, Birkhäuser, 1996.

[3] A. Bigatti and E. Sáenz-de-Cabezón, Computation of the $(n-1)$-st Koszul Homology of monomial ideals and related algortihms, Procedings of the International Symposium on Symbolic and Algebraic Computation, 2009, pp. 31-37

[4] E. Sáenz-de-Cabezón, Multigraded Betti numbers without computing minimal free resolutions, Applicable Algebra in Enginereing, Communications and Computing, 20(5-6) 2009, pp.481-495

Multidimensional persistence and directed topology

J. Dubut[1,2], E. Goubault[2], J. Goubault-Larrecq[1]

[1] *LSV, ENS Cachan, CNRS, Université Paris-Saclay, F-94230 Cachan, {dubut, goubault}@lsv.ens-cachan.fr*
[2] *LIX, Ecole Polytechnique, CNRS, Université Paris-Saclay, F-91128 Palaiseau Cedex, {goubault, dubut}@lix.polytechnique.fr*

1 Directed topology, concurrency and homology

Introduction. *Directed* algebraic topology is a variant of algebraic topology where the spaces also have a direction of time [12, 8], and deformations must not only be continuous but also preserve the direction of time. Directed algebraic topology was born out of the so-called geometric semantics of concurrent processes (progress graphs [3]), and the higher-dimensional automaton model of true concurrency [14]. Imagine n concurrent processes, each with a local time $t_i \in [0,1]$. A configuration is a point in $[0,1]^n$, and a trajectory is a continuous *and monotonic* map from $[0,1]$ to $[0,1]^n$: monotonicity (a.k.a., directedness) reflects the fact that no process can go back in time. One can arguably consider as equivalent any two trajectories that are dihomotopic, namely that can be deformed into each other continuously, while respecting monotonicity at all times. This not only yields a geometric semantics for concurrency, but also one that is at the root of fast algorithms for state-space reduction, deadlock and unreachable states detection, and verification of coordination properties, as in e.g. [9, 7, 10, 11].

Technical context of the talk. The link between directed algebraic topology, and more particularly natural homology [4], with multidimensional persistent homology will be exemplified, for the sake of simplicity, on a simple class of directed spaces, the cubical complexes of [13, 4].

A cubical complex is a finite union of certain cubes of various dimensions, but always of side-length 1 parallel to the axes in $\mathbb{R}^d$, whose vertices have integer coordinates. These cubical complexes K can also be seen as (pre-)cubical sets with the obvious boundary operators, and as po-spaces $(K, \leq)$, the simplest form of directed spaces, where the global partial order $\leq$ expressing the time flow is given by the componentwise ordering on $\mathbb{Z}^d$.

A *dipath* is a path which is also monotonic in the ordering of the cubical complex. Following Raussen [15], a (directed) *trace* is the equivalence class $\langle \pi \rangle$ of a dipath π modulo monotonic and continuous reparametrization, and the set of such

equivalence classes can be given the structure of a topological space $Tr(K;a,b)$ for all start (resp. end) points a (resp. b).

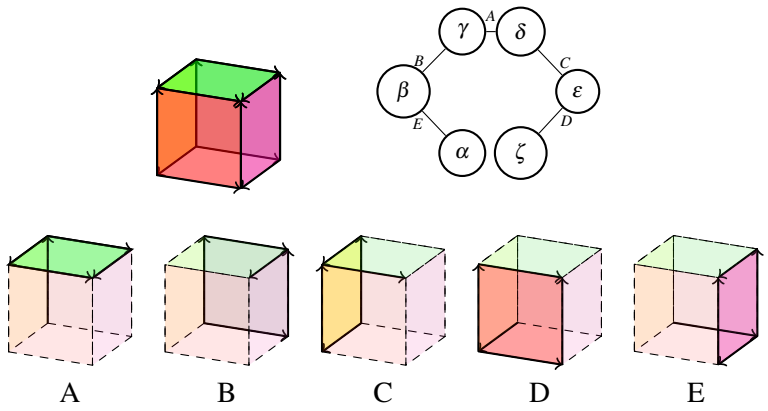
Directed algebraic topology is the study of directed spaces as our cubical complexes, up to directed homeomorphisms, or some form of homotopy equivalence [5]. An invariant of these directed spaces [15] is an invariant for classical homotopy of the traces spaces $Tr(K;a,b)$, for all points $a,b \in K$, and, even, the full "diagram" (modulo some form of bisimulation) of spaces $Tr(K;a,b)$ when a and b evolve in K, meaning that we are also interested in maps $Tr(K;a,b) \to Tr(K;a',b')$ ($a' \leq a$ and $b \leq b'$) and of their (classical) homotopy types. We refer the reader to [4] for more explanations and a complete formalization of these ideas in the form of a natural system [1] of topological spaces : we defined the n-th directed homology group $\overrightarrow{H}_n(X;a,b)$ as the ordinary $(n-1)$st singular homology group of $Tr(X;a,b)$, and the diagram of such for a and b varying (over the grid $K \cap \mathbb{Z}^d$) is the natural homology of K denoted by $\overrightarrow{H}_*(K)$.

2 Natural homology and multi-dimensional persistence

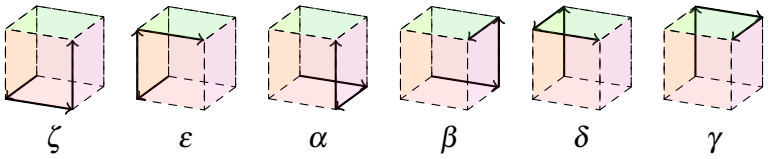
Main results. For finite K, Raussen [16] shows that singular homology groups of trace spaces such as $Tr(K;a,b)$ are computable, by computing a finite presentation of the trace spaces (prod-simplicial complex) from which we can compute homology using Smith normal form of matrices. The problem is that this construction is not nicely behaved in general with respect to changes of base points a, b.

For "nice" precubical sets X (such as our cubical complexes K), and for any vertices a and b in X, there is a way to get a finite combinatorial model $T(X)(a,b)$ (a finite CW-complex, or a finite simplicial set) that is homotopy equivalent to the trace space of X from a to b, $Tr(X;a,b)$, which is both functorial in X, a, b and also minimal among such functors [17]. We will show in the talk how to use this ingredient together with some of the multidimensional persistence theory, such as rank invariants [2], to get information (in fact, all the information, in many cases) about natural homology, and develop the corresponding algorithmics.

Example. To give a glimpse of the intimate relationship between multidimensional persistence and natural homology, let us describe our construction on Fahrenberg's matchbox example [6], left below (all but the bottom face of the unit cube $[0,1] \times [0,1] \times [0,1]$ is in the cubical complex - i.e. there are 5 squares glued together). Using Ziemiański's construction [17], the CW-complex/simplicial set corresponding to its trace space from beginning to end is shown below, where the edges A, B, C, D and E correspond to the 5 2-dimensional cubical paths shown in the picture below :

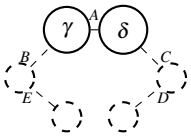
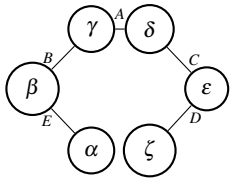
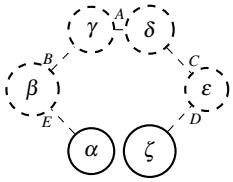


and the vertices α, β, γ, δ, ε and ζ correspond to the 6 1-dimensional dipaths :



Note that β is the geometric intersection of B with E, γ is the geometric intersection of B with A etc. leading indeed to the simplicial set pictured right-hand side of the first figure. Now, by functoriality of T in the start and end points, there are maps from $T(K)(a,b)$ to $T(K)(a',b')$, for $a \leq a'$ and $b' \leq b$ that act as restriction maps : they just "cut" the combinatorial dipaths so as to only keep the parts (if any) that go from a' to b'. Hence, we get a decreasing sequence of simplicial sets as soon as any of the three coordinates of a increase or any of the three coordinates of b decrease. Below, we have represented the part of the multidimensional filtration generated, for the vertical coordinate of b (the end point) and of a (the starting point) ; recall also that the 5 squares are here unit squares and the lower coordinates are 0, upper ones are 1. In this filtration below, the restriction maps acting on combinatorial dipaths generate inclusion maps from bottom to top, and from left to right, of simplicial sets representations of the corresponding trace spaces. For instance, moving the end point b from vertical coordinate 1 to 0 while keeping vertical coordinate of a at 0 (right column in the table below), the only 1-dimensional paths going through coordinate 0 for b are α and ζ, hence all other vertices (and edges) have to disappear from the simplicial set representation of the trace space. This induces the upwards inclusion map from the two points simplicial set (α and ζ) into the 5 edges connected simplicial set above : H_0 of these simplicial sets goes from $\mathbb{Z}^2$ to $\mathbb{Z}$, "killing" one component when extending paths to reach the end point of the matchbox. This corresponds, in the natural homology diagram $\overrightarrow{H}_1(K)$, to part of

the diagram being a projection map from $\mathbb{Z}^2$ to $\mathbb{Z}$ when moving b to the endpoint of the matchbox, while keeping the starting point fixed at the initial vertex :

b/a	1	0
1		
0	∅	

Algorithms. In the talk, we will also discuss many of the algorithmic issues. A major one is how to generate efficiently the simplicial sets above, and get efficiently a representation of the boundary maps as matrices with (multivariate) polynomial coefficients. Finally, we introduced in [4] a notion of bisimulation of diagrams, so that different "encodings" of the time coordinates (corresponding to the coordinates in the multifiltration) of shapes which should be directed homotopy equivalent, give bisimilar diagrams in (natural) homology. This is akin to interleaving distances methods in persistence, but their exact relationship is not yet fully understood.

References

[1] H.-J. Baues and G. Wirsching. Cohomology of small categories. *Journal of Pure and Applied Algebra*, 38(2-3):187–211, 1985.

[2] G. E. Carlsson, G. Singh, and A. Zomorodian. Computing multidimensional persistence. *CoRR*, abs/0907.2423, 2009.

[3] E. G. Coffman, M. J. Elphick, and A. Shoshani. System deadlocks. *Computing Surveys*, 3(2):67–78, 1971.

[4] J. Dubut, E. Goubault, and J. Goubault-Larrecq. Natural homology. In *ICALP*, pages 171–183, 2015.

[5] J. Dubut, E. Goubault, and J. Goubault-Larrecq. The directed homotopy hypothesis. In *CSL*, 2016.

[6] U. Fahrenberg. Directed homology. *Electronic Notes in Theoretical Computer Science*, 100:111–125, 2004.

[7] L. Fajstrup, E. Goubault, E. Haucourt, S. Mimram, and M. Raußen. Trace Spaces: An Efficient New Technique for State-Space Reduction. In *ESOP*, 2012.

[8] L. Fajstrup, E. Goubault, E. Haucourt, S. Mimram, and M. Raussen. *Directed Algebraic Topology and Concurrency*. Springer, 2016.

[9] E. Goubault. Geometry and concurrency: A user's guide. *Mathematical Structures in Computer Science*, 10(4):411–425, 2000.

[10] E. Goubault and E. Haucourt. A Practical Application of Geometric Semantics to Static Analysis of Concurrent Programs. In *16th Intl. Conf. Concurrency Theory (CONCUR)*, pages 503–517, 2005.

[11] E. Goubault, T. Heindel, and S. Mimram. A geometric view of partial order reduction. *ENTCS*, 298, 2013.

[12] M. Grandis. *Directed Algebraic Topology, Models of non-reversible worlds*. Cambridge University Press, 2009.

[13] T. Kaczynski, K. Mischaikow, and M. Mrozek. Computing homology. *Homology, Homotopy and Applications*, 5(2):233–256, 2003.

[14] V. R. Pratt. Modeling Concurrency with Geometry. In *POPL*, pages 311–322, 1991.

[15] M. Raussen. Invariants of directed spaces. *Applied Categorical Structures*, 15, 2007.

[16] M. Raussen. Simplicial models for trace spaces II: General higher dimensional automata. *Algebraic and Geometric Topology*, 12(3), 2012.

[17] K. Ziemiański. Spaces of directed paths on pre-cubical sets. *Applicable Algebra in Engineering, Communication and Computing*, 2017.

Combinatorial Multivector Fields

M. Juda[1], joint work with: Marian Mrozek, Tamal Dey, Tomasz Kapela, Mateusz Przybylski.

[1] *Jagiellonian University, Poland; mateusz.juda@uj.edu.pl;* *This research is supported by the Polish NCN under Maestro Grant No. 2014/14/A/ST1/00453*

In this talk we show a combinatorial approach to analyze vector field data sets. The aim of the method is to work on dynamical systems given as data sets obtained from numerical or physical experiments however, without any assumptions about the differential equation model. We provide topological characterization of attractors and repellers, Conley indices, and Morse decomposition. The work is based on [1] and our recent results.

Our method accept an input consisted of a point cloud data with a vector attached at each point. Using the points we build a combinatorial structure X of the phase space (simplicial complex, e.g. Delaunay triangulation). Next we extend the vector field to each cell of the complex X in a following way. For each cell σ in dimension greater than 0 we compute a vector v_σ which is equal to the average of the vectors attached to each vertex of σ. Then we use v_σ to define a map $m : X \to X$. The value of $m(\sigma)$ is a coface of σ, which is a target of v_σ. Usually it is a top dimensional coface of σ. However, for vertices we use a parameter α which describes closeness of v_σ to its cofaces. Let $T := \{\tau_1, \tau_2, \ldots, \tau_k\}$ be a subset of cofaces of σ such that the angle between v_σ and τ_i is less than α. Then we select τ_i with smallest dimension among cells in T and set $m(\sigma) := \tau_i$. See Figure 1 as an example.

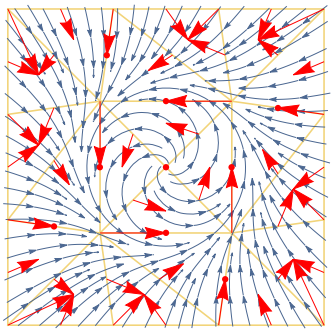


Figure 1: A vector field extended to a mesh. Yellow lines show the simplicial complex triangles, blue arrows show a stream plot of a dynamical system (which is not known for the method). Red arrows show the mapping $m(\sigma)$. Red arrows which points into an edge are flattened according to the rule described above and a value of the parameter α.

Afterwards we generalize Forman's theory of combinatorial vector fields [2].

Namely, we build a partition of the space X into *multivectors* - convex subsets of X - using the mapping m. The partition leads us to combinatorial description of the vector field dynamics, i.e. we get a directed graph which encodes the dynamics. Strongly connected components of the graph give us Morse decomposition of the dynamical system.

Depends on the value of α we get different approximation of the dynamics given by the vector field. For the Van der Pol equation:

$$f(x_0, x_1) = (-x_1, (x_0^2 - 1) * x_1 + x_0)$$

we show Morse sets obtained for $\alpha = 60^\circ$ and $\alpha = 18^\circ$ in Figure 2 and in Figure 3 accordingly.

Varying values of the α parameter allows us to define *persistence* of the Morse sets. Namely, we describe structure of the Morse sets using finite topological spaces theory [3]. Afterwards we can define ZigZag filtration [4] and compute persistence barcodes of the Morse sets. Figure 4 show barcodes for the Van der Pol system.

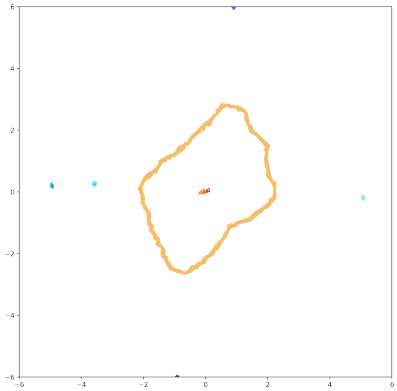


Figure 2: Morse sets for the Van der Pol equation, $\alpha = 60^\circ$. Orange set represents the repeling periodic orbit of the system. In the center there is a Morse set for the attracting point. Other sets are present due to artifacts of the method.

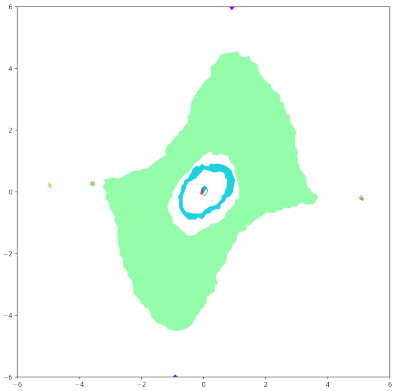


Figure 3: Morse sets for the Van der Pol equation, $\alpha = 18^\circ$. Green set represets the repeling periodic orbit of the system. Blue set is another periodic orbit however, it is with trivial Conley index. In the center there is a Morse set for the attracting point. Other sets are present due to artifacts of the method.

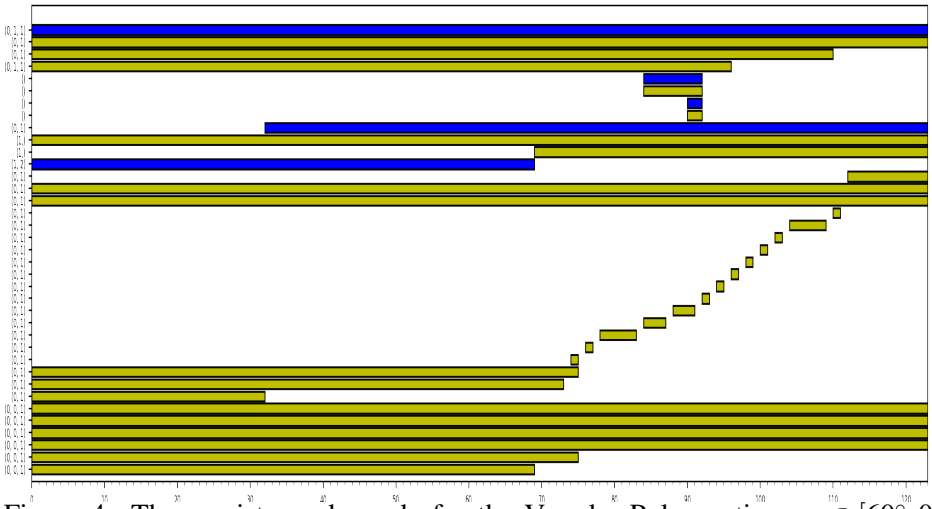


Figure 4: The persistence barcode for the Van der Pol equation, $\alpha \in [60°, 0°]$. Yellow bars for homology generators in dimension 0, blue bars for dimension 1. Labels on the left side show Conley indices of the Morse sets.

References

[1] M. Mrozek, *Conley-Morse-Forman Theory for Combinatorial Multivector Fields on Lefschetz Complexes*, M. Found Comput Math (2016).

[2] R. Forman, *Morse Theory for Cell Complexes*, Advances in Mathematics, Volume 134, Issue 1, 1998, Pages 90-145, ISSN 0001-8708, http://dx.doi.org/10.1006/aima.1997.1650

[3] M. McCord, *Singular homology groups and homotopy groups of finite topological spaces*, Duke Math. J. 33 (1966), no. 3, 465–474. doi:10.1215/S0012-7094-66-03352-7.

[4] G. Carlsson, V. Silva, D. Morozov, *Zigzag persistent homology and real-valued functions*, Proceedings of the twenty-fifth annual symposium on Computational geometry (2009), 247–256.

Distributed computation of low-dimensional cup products

N. Alokbi[1] & G. Ellis[2]

[1] *National University of Ireland, Galway*
[2] *National University of Ireland, Galway* graham.ellis@nuigalway.ie

We describe a distributed algorithm for computing the cup product $\cup: H^1(X,\mathbb{Z}) \times H^1(X,\mathbb{Z}) \to H^2(X,\mathbb{Z})$ on the cohomology of a finite regular CW-space. A serial implementation of the algorithm is illustrated in two applied topological settings: (i) 3-dimensional digital images; (ii) topological data analysis of a finite sample of points from a metric space. For the second of these illustrations we introduce a cohomological enrichment of the Mapper clustering procedure which may be of independent interest.

Computation of AT-models based on exploratory trees

P. Real

[1] *Institute of Mathematics, University of Sevilla (Spain), real@us.es.*

This research is supported by the Spaniard (AEI/FEDER, UE) research project MTM2016-81030-P.

Working with coefficients in a field, we design algorithmic work for developing homology computation within the AT-model (Algebraic Topological model) setting [2, 1, 3, 5, 4]. More precisely, given a finite (abstract) cell complex X, we design a polynomial algorithm computing an AT-model based on exploratory trees over a subdivision of X. Instead of computing an AT-model of X using a previous filtration over it or the classical Smith normal form diagonalization of incidency matrices, we use a pre-processing method for decomposing the incidency graph of X into a suitable hierarchical set of "maximal" connectivity trees over the dual intersection subdivision of X. This work is a continuation of the study done in [6].

References

[1] González-Díaz, R., Medrano, B., Sánchez-Peláez, J. and Real, P. (2006, September). *Simplicial perturbation techniques and effective homology*. In International Workshop on Computer Algebra in Scientific Computing (pp. 166-177). Springer Berlin Heidelberg.

[2] González-Díaz, R. and Real, P. (2005). *On the cohomology of 3D digital images*. Discrete Applied Mathematics, 147(2), 245-263.

[3] Molina-Abril, H. and Real, P. (2012). *Homological optimality in Discrete Morse Theory through chain homotopies*. Pattern Recognition Letters, 33(11), 1501-1506.

[4] Palmieri J. H. (2015). *Module "Algebraic Topological Model for a Cell Complex" of "Geometry and Topology:Cell Complexes and its homology"*. Sage: Open source mathematical software (http://doc.sagemath.org/)

[5] Pilarczyk, P. and Real, P. (2015). *Computation of cubical homology, cohomology, and (co) homological operations via chain contraction*. Advances in Computational Mathematics, 41(1), 253-275.

[6] Real Jurado, P., Molina-Abril, H., González-Lorenzo, A., Bac, A. and Mari, J. L. (2015). *Searching combinatorial optimality using graph-based homology information*. Applicable Algebra in Engineering, Communication and Computing, Vol. 26, Issue 1, pp 103-120.

Modeling and replicating statistical topology, and evidence for CMB non-homogeneity

R.J. Adler[1], S. Agami[1], Pratyush Pranav[1]

[1] *Andrew and Erna Viterbi Faculty of Electrical Engineering*
Technion – Israel Institute of Technology

Under the banner of 'Big Data', the detection and classification of structure in extremely large, high dimensional, data sets, is, one of the central statistical challenges of our times. Among the most intriguing approaches to this challenge is 'TDA', or 'Topological Data Analysis', one of the primary aims of which is providing non-metric, but topologically informative, pre-analyses of data sets which make later, more quantitative analyses feasible. While TDA rests on strong mathematical foundations from Topology, in applications it has faced challenges due to an inability to handle issues of statistical reliability and robustness and, most importantly, in an inability to make scientific claims with verifiable levels of statistical confidence. We propose a methodology for the parametric representation, estimation, and replication of persistence diagrams, the main diagnostic tool of TDA. The power of the methodology lies in the fact that even if only one persistence diagram is available for analysis – the typical case for big data applications – replications can be generated to allow for conventional statistical hypothesis testing. The methodology is conceptually simple and computationally practical, and provides a broadly effective statistical procedure for persistence diagram TDA analysis. We present extensive illustration of our methodology, and at the end we present the power of the approach in a novel and revealing analysis of CMB non-homogeneity.

Session 3

Computer differential and difference algebra and its applications

Session chairs:

Vladimir Gerdt
LIT, JINR, Dubna, Russia

Alexander Levin
CUA, Washington D.C., USA

Daniel Robertz
University of Plymouth, UK

Generalized Weyl algebras and diskew polynomial rings

V. V. Bavula

University of Sheffield, Sheffield, UK, v.bavula@sheffield.ac.uk

The aim of the talk is to introduce two new classes of rings – *generalized Weyl algebras* and *diskew polynomial rings* - to consider their properties and to give several simplicity criteria for them. The first class is a generalization of the classical generalized Weyl algebras. Examples are given.

Differential algebra with mathematical functions, symbolic powers, and anticommutative variables

E.S. Cheb-Terrab[1]

[1] *Maplesoft R&D, Canada, ecterrab@maplesoft.ca*

Computer algebra implementations of Differential Algebra typically require that the systems of equations to be tackled be rational in the independent and dependent variables and their partial derivatives. It is possible, however, to extend this computational domain and apply Differential Algebra techniques to systems of equations that involve arbitrary compositions of mathematical functions (elementary or special), fractional and symbolic powers, as well as anticommutative variables and functions. In this talk, this extension of the computational domain of Differential Algebra is explained, and examples of its implementation in the Maple computer algebra system, as well as of its use in the Maple ODE and PDE solvers, are shown.

The key observation regarding performing standard differential algebra operations on expressions that include mathematical functions is the fact that, but for rather few exceptions, they belong to a set of functions whose derivatives belong to the same set. For example, the derivative of a hypergeometric function is also a hypergeometric function, and with that the derivatives of all elementary and special functions that are particular cases of hypergeometric functions happen to belong to the same set as the functions themselves. It is then possible to represent each mathematical function of this group by an auxiliary function F_i that satisfies a differential equation, rational in the F_i, their derivatives and the independent variables (the mathematical functions' parameters). In brief, in the original system that includes mathematical functions, each of them is replaced by an auxiliary F_i, the differential equation it satisfies is added to the system, the differential algebra operations are performed, and at the end the F_i are substituted back by the mathematical functions they represent. As the simplest example of this, a system involving the exponential function of x is one where this function can be replaced by F and the equation $F' = F$ added to the system.

This rewriting of the original system by replacing mathematical functions by the F_i plus adding the rational differential equations they satisfy is called *rewriting the original system in differential polynomial form*, and the whole problem of performing differential algebra operations on systems that involve mathematical functions is thus reduced to this rewriting.

Returning to the representation problem, symbolic powers, say $F = x^n$, in turn satisfy $xF' - nF = 0$, and it is not difficult to see that the case where the mathematical function's arguments are not simple variables x_i, for example an exponential

function of the form $e^{f(x)}$, can also be tackled as just described but for the addition of a change of variables to handle $f(x)$, provided that $f(x)$ itself can be written in differential polynomial form. In this way, for example, we find that $F = e^{x^n}$ satisfies $F''Fx-(F'x+F(n-1))F' = 0$.

This approach can be used as well for *derivatives evaluated at a point*, which appear frequently in the symbolic (exact) solution of systems of partial differential equations tackled using changes of variables, a standard operation in most methods, including the Lie symmetry and integrating factor approaches. Indeed, by differentiating one can see that, depending on the evaluation point, the derivative can be differentiated resulting again in closure (the objects and their derivatives happen to belong to the same set and therefore are suitable for a differential polynomial representation). For example, the function $F(x,t) = D(f)(x-t)+D(f)(x+t)$, where D is a differential operator and f is a mapping of one argument (a function of one variable), by means of this approach can be represented in differential polynomial form as $F_{xx}-F_{tt} = 0$. In the same way, one can represent integrals, provided that the integrand admits differential polynomial form; and in general, any arbitrary mathematical composition of operations (mathematical functions, symbolic powers, derivatives, integrals, etc.) with no restrictions to the levels of nesting, can be represented in differential polynomial form provided that the arguments of those operations in turn admit such rewriting.

Finally, the case of a PDE system involving anticommutative variables and functions can be reduced to the previous problem by expanding these functions in powers of the anticommutative variables. In view of the anticommutative character, these expansions truncate at first order in each anticommutative variable, so that each equation of the original system splits into equations without anticommutative variables, which can then be rewritten in differential polynomial form, tackled using differential algebra techniques, and at the end, the resulting equations can be recast as a system in the original anticommutative variables. As an example of an ODE involving anticommutative variables tackled using differential algebra techniques, consider Q as an anticommutative function, so that $Q^2 = 0$, then the ODE $Q''-QQ' = 0$ has for solution $Q = (c_1x+c_2)\lambda$, where λ is an anticommutative arbitrary constant. For a PDE example, consider an anticommutative function $Q(x,y,\theta)$ where Q and θ are anticommutative, then $Q_{x\theta} = 0$ has for solution $Q(x,y,\theta) = F_1(x,y)\lambda+F_2\theta$, where F_1 and F_2 are arbitrary commutative functions.

References

[1] J.F. Ritt, *Differential Algebra*, American Mathematical Society, Colloquium publications Vol.33 (1950).

On finite difference approximations to the Korteveg-de Vries equation and its conservation laws

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 real constants. Based on the methodology of paper [1], we suggested in [2] an approach to algorithmic generation of finite difference approximations to the nonlinear evolution equations of the form

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

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

The class (1) contains the classical Korteveg-de Vries (KdV) equation which we shall write as

$$f = 0\,, \quad f := u_t + \alpha\, u\, u_x + \beta\, u_{xxx}\,, \quad u = u(t,x)\,, \quad \alpha,\beta \in \mathbb{R}\,. \tag{2}$$

The finite difference approximation (FDA) to Eq. (2), generated by the procedure described in [2] and based on application of difference Gröbner bases [3] reads

$$\begin{aligned} &\tilde{f} = 0\,, \quad \tilde{f} := \frac{u_j^{n+1}-u_j^n}{\tau} + \alpha\frac{(P_{j+1}^{n+1}-P_{j-1}^{n+1})+(P_{j+1}^n-P_{j-1}^n)}{8h} \\ &+\beta\,\frac{(u_{j+2}^{n+1}-2u_{j+1}^{n+1}+2u_{j-1}^{n+1}-u_{j-2}^{n+1})+(u_{j+2}^n-2u_{j+1}^n+2u_{j-1}^n-u_{j-2}^n)}{4h^3}\,. \end{aligned} \tag{3}$$

where $u_j^n := u(\tau\cdot n, h\cdot j)$ $(n,j \in \mathbb{Z})$ is the grid function which approximates $u(t,x)$ on the Cartesian solution grid with spacings $\tau := t_{n+1}-t_n, h := x_{j+1}-x_j$ and $P_j^n := (u^2)_j^n$, . The FDA (3) has accuracy $O(\tau^2,h^2)$ and is *consistent* with (2). Besides, as a difference scheme, it is implicit, and hence unconditionally *stable*. Therefore, the scheme (3) is *convergent*.

Apparently, the differential ideal $[\![f]\!]$, generated by f in (2), is radical, and the difference ideal $[\![\tilde{f}]\!]$, generated by $\tilde{f}$ in (3), is a perfect one (cf. [4]) in the inversive difference ring $\mathbb{Q}(\alpha,\beta)\{u\}$ with differences σ_t, $\sigma_x, \sigma_t^{-1}, \sigma_x^{-1}$ acting as

$$\sigma_t \circ u_j^n = u_j^{n+1}\,, \;\; \sigma_x \circ u_j^n = u_{j+1}^n\,, \;\; \sigma_t^{-1} \circ u_j^n = u_j^{n-1}\,, \;\; \sigma_x^{-1} \circ u_j^n = u_{j-1}^n\,.$$

Since $\tilde{f}$ is a Gröbner basis of $[\![\tilde{f}]\!]$, the consistency implies *s(strong)-consistency* [5] by the following theorem.

Theorem 1 [5] *A FDA $\tilde{F}$ to a (system of) differential polynomial(s) F is s-consistent iff every element in the Gröbner (standard) basis of the difference ideal generated by $\tilde{F}$ provides FDA to an element of the radical differential ideal generated by F.*

The property of s-consistency of $\tilde{f}$ with f means that any element in $[\![\tilde{f}]\!]$ is a FDA to an element in $[\![\tilde{f}]\!]$. Among elements in $[\![\tilde{f}]\!]$ there are infinitely many (local) *conservation laws*

$$\{\, \mathfrak{C}_i := \partial_t T_i + \partial_x X_i \in [\![f]\!] \Longrightarrow \frac{d}{dt}\int_{-\infty}^{\infty} T_i\, dx = -[X_i]_{-\infty}^{\infty} \mid i \in \mathbb{N}_{\geq 1}\,,\ T_i, X_i \in \mathscr{R}\}$$

where $T_i = T_i(u)$ are *densities* and $X_i = X_i(u)$ are *fluxes*.

The conservation laws of KdV admit algorithmic construction. There are computer algebra packages, e.g. the Maple package PDEBELLII [6], which recursively compute T_i and X_i. Then one can express $\mathfrak{C}_i$ via f with a help of the Maple package the DIFFERENTIALTHOMAS implementing differential Thomas decomposition [7]. The first five conservation laws presented in Table 1.

Table 1: Low order conservation laws of KdV in terms of f

i	$\mathfrak{C}_i$	$\mathrm{ord}_x(\mathfrak{C}_i)$
1	f	3
2	f_x	4
3	$f_{xx} + 2uf$	5
4	$f_{xxx} + uf_x^4 + u_x^4 f$	6
5	$f_{xxxx} + 6uf_{xx} + 5u_x f_x + 6u_{xx} f + 6u^2 f$	7
...	.....	.....

Exact or approximate inheritance of conservation laws at the discrete level is one of the most important qualitative requirements to finite difference schemes [8]. Due to the s-consistency with (2), the discretization (3) approximately inherits all its conservation laws as the following theorem states. It is the main theoretical result of this note.

Theorem 2 *For each conservation law $\mathfrak{C}_i$ of KdV there is an element $\tilde{f}_i$ in the perfect difference ideal $[\![\tilde{f}]\!]$ such that $\tilde{f}_i$ approximates $\mathfrak{C}_i$ with the accuracy $O(\tau^2, h^2)$ corresponding to the accuracy of $\tilde{f}$.*

We illustrate this fact by the 3rd and 4th KdV conservation laws of Table 1. With regard to *forward and backward differences*

$$\Delta_p := \frac{1}{h}(\sigma_x - 1), \qquad \Delta_m := \frac{1}{h}(1 - \sigma_x^{-1}),$$

the spatial derivatives occurring in $\mathfrak{C}_3$ and $\mathfrak{C}_4$ are approximated, with the prescribed accuracy, by the elements in $\mathscr{R}$ and $[\![\tilde{f}]\!]$ as follows

$$\frac{1}{2}(\Delta_p + \Delta_m) \circ u \xrightarrow[h\longrightarrow 0]{} u_x + O(h^2), \quad \frac{1}{2}(\Delta_p + \Delta_m) \circ \tilde{f} \xrightarrow[h\longrightarrow 0]{} f_x + O(h^2),$$

$$\Delta_m \Delta_p \circ \tilde{f} \xrightarrow[h\longrightarrow 0]{} f_{xx} + O(h^2), \ \ \Delta_p \Delta_m \Delta_p \circ \tilde{f} - \frac{h}{2}\Delta_m \Delta_p \Delta_m \Delta_p \circ \tilde{f} \xrightarrow[h\longrightarrow 0]{} f_{xxx} + O(h^2).$$

We correlated numerical behavior of our scheme (3) with two other schemes taken from the book [9]. Both of them have the same accuracy $O(\tau^2, h^2)$ as (3).

Explicit Scheme I ([9], Eq.1.80)

$$u_i^{n+1} = u_i^{n-1} - \frac{\alpha\tau}{h} u_i^n \left(u_{i+1}^n - u_{i-1}^n\right) - \frac{\beta\tau}{h^3}\left(u_{i+2}^n - 2u_{i+1}^n + 2u_{i-1}^n - u_{i-2}^n\right).$$

stable for

$$\tau \le \frac{2h^3}{3\sqrt{3}\beta} \cong 0.384\frac{h^3}{\beta}.$$

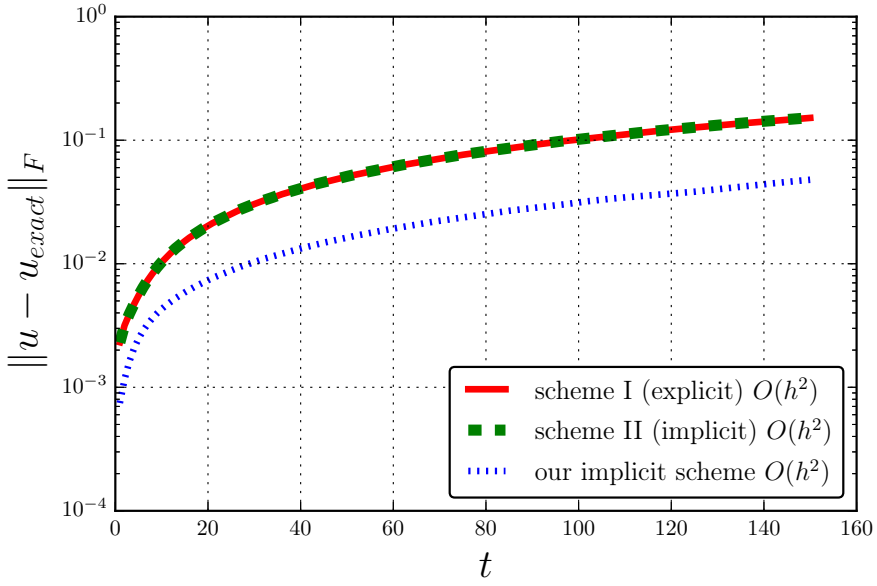
Implicit Scheme II ([9], Eq.1.96)

$$\frac{u_j^{n+1} - u_j^n}{\tau} + \frac{\alpha}{4h}\left[u_j^n\left(u_{j+1}^{n+1} - u_{j-1}^{n+1}\right) + u_j^{n+1}\left(u_{j+1}^n - u_{j-1}^n\right)\right] +$$
$$+ \frac{\beta}{4h^3}\left(\left(u_{j+2}^{n+1} - 2u_{j+1}^{n+1} + 2u_{j-1}^{n+1} - u_{j-2}^{n+1}\right) + \left(u_{j+2}^n - 2u_j^{n+1} + 2u_{j-1}^n - u_{j-2}^n\right)\right) = 0.$$

As a benchmark, we used the exact one-soliton solution

$$u_{\text{exact}}(x,y) = \frac{2k_1^2}{\cosh(k_1(x - 4k_1^2 t))^2}$$

to (2) with $\alpha = 6$, $\beta = 1$ and $k_1 = 0.4$. In so doing, we fixed $h = 0.25$ and considered the solution in interval $-50 \le x \le 50$ with periodic boundary conditions (cf. [9], p.49). The numerical inaccuracy was estimated by the Frobenius norm. The following picture shows numerical superiority of our scheme.



References

[1] 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, 2:26, 2006. arXiv:math.RA/0605334

[2] Yu. A. Blinkov, V. P. Gerdt and K. B. Marinov: Computer Algebra Based Discretization of Quaslinear Evolution Equations. Programming and Computer Software, 43(2), 2017, 84–89.

[3] V. P. Gerdt and D. Robertz: Computation of Difference Gröbner Bases. Computer Science Journal of Moldova, 20(2), 2012, 203–226. arXiv:cs.SC/1206.3463

[4] A. Levin: Difference Algebra. Algebra and Applications, Vol.8. Springer, New York, 2008.

[5] V. P. Gerdt: Consistency Analysis of Finite Difference Approximations to PDE Systems. Proceedings of MMCP 2011 (July 3-8, 2011, Stará Lesná, High Tatra Mountains, Slovakia), G.Adam, J.Buša, M.Hnatič (Eds.), LNCS 7125, Springer-Verlag, Berlin, 2012, pp.28–42. arXiv:math.AP/1107.4269

[6] Qian Miao, Yunhu Wang, Yong Chen and Yunqing Yang. PDEBellII: A Maple package for finding bilinear forms, bilinear Bäcklund transformation, Lax pairs and conservation laws of the KdV-type equations. Computer Physics Communications, Vol. 185, 2014, 357–367.

[7] T. Bächler, V. Gerdt, M. Lange-Hegermann and D. Robertz: Algorithmic Thomas decomposition of algebraic and differential systems. Journal of Symbolic Computation, 47(10), 2012, 1233–1266. arXiv:math.AC/1108.0817

[8] J. E. Castillo and G. F. Miranda. Mimetic Discretization Methods. CRC Press, Boca Raton, 2013.

[9] V. Yu. Belashov and S. V. Vladimirov: Solitary Waves in Dispersive Complex Media. Theory · Simulation · Applications. Springer-Verlag, Berlin, 2005.

Bivariate Dimension Quasi-polynomials of Difference-Differential Field Extensions with Weighted Basic Operators

Alexander Levin

The Catholic University of America, Washington, D.C., USA, levin@cua.edu

We prove the existence and determine some invariants of a Hilbert-type bivariate quasi-polynomial associated with a difference-differential field extension with weighted basic derivations and translations. We show that such a quasi-polynomial can be expressed in terms of univariate Ehrhart quasi-polynomials of rational conic polytopes.

1. Preliminaries

Let K be a 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 mappings from the set $\Delta \cup \sigma$ commute) and let every δ_i, $1 \leq i \leq m$ (respectively, every α_j, $1 \leq j \leq n$), be assigned a positive integer weight v_i (respectively, w_j). Let Λ be the free commutative semigroup generated by the set $\Delta \cup \sigma$ whose elements are written as power products $\lambda = \delta_1^{k_1} \dots \delta_m^{k_m} \alpha_1^{l_1} \dots \alpha_n^{l_n}$ ($k_i, l_j \in \mathbb{N}$).

We define the orders of λ with respect to the sets Δ and σ (and with respect to the given weights) as $\mathrm{ord}_\Delta \lambda = \sum_{i=1}^m v_i k_i$ and $\mathrm{ord}_\sigma \lambda = \sum_{j=1}^n w_j l_j$, respectively, and set $\Lambda_{V,W}(r,s) = \{\lambda \in \Lambda \mid \mathrm{ord}_\Delta \lambda \leq r, \mathrm{ord}_\sigma \lambda \leq s\}$ for all $r, s \in \mathbb{N}$.

In what follows, we will use the prefix Δ-σ- instead of the adjective "difference-differential". If $\eta = \{\eta_1, \dots, \eta_q\}$ is a finite subset of a Δ-σ-overfield of K, we write $K\langle \eta_1, \dots, \eta_q \rangle$ for the Δ-σ-field extension of K generated by the set η. (As a field, it coincides with $K(\{\lambda(\eta_i) \mid \lambda \in \Lambda, 1 \leq i \leq q\})$.)

2. Dimension quasi-polynomials of subsets of $\mathbb{N}^p$

A function $f : \mathbb{Z} \to \mathbb{Q}$ is called a (univariate) *quasi-polynomial* of period q if there exist q polynomials $g_i(x) \in \mathbb{Q}[x]$ $(0 \leq i \leq q-1)$ such that $f(n) = g_i(n)$ whenever $n \in \mathbb{Z}$ and $n \equiv i \,(mod\, q)$.

An equivalent way of introducing quasi-polynomials is as follows.

A *rational periodic number* $U(n)$ is a function $U : \mathbb{Z} \to \mathbb{Q}$ with the property that there exists (a period) $q \in \mathbb{N}$ such that $U(n) = U(n')$ whenever $n \equiv n' \,(mod\, q)$.

A rational periodic number can be represented by a list of q its possible values: $U(n) = [a_0, \dots, a_{q-1}]_n$. For example, $U(n) = \left[\frac{1}{2}, \frac{3}{4}, 1\right]_n$ is a periodic number with period 3 such that $U(n) = \frac{1}{2}$ if $n \equiv 0 \,(mod\, 3)$, $U(n) = \frac{3}{4}$ if $n \equiv 1 \,(mod\, 3)$, and $U(n) = 1$ if $n \equiv 2 \,(mod\, 3)$.

With the above notation, a (univariate) *quasi-polynomial of degree d* is a function $f : \mathbb{Z} \to \mathbb{Q}$ such that

$$f(n) = c_d(n)n^d + \cdots + c_1(n)n + c_0(n)$$

where $c_i(n)$'s are rational periodic numbers and $c_d(n) \neq 0$ for at least one $n \in \mathbb{Z}$.

One of the main applications of the theory of quasi-polynomials is its application to the counting of integer points in polytopes.

Recall that a *rational polytope* in $\mathbb{R}^d$ is the convex hall of finitely many points (vertices) in $\mathbb{Q}^d$ or, equivalently, the set of solutions of a finite system of linear inequalities $A\mathbf{x} \leq \mathbf{b}$, where A is an $l \times d$-matrix with integer entries (l is a positive integer) and $\mathbf{b} \in \mathbb{Z}^l$, provided that the solution set is bounded.
Let $P \subseteq \mathbb{R}^d$ be a rational polytope. In what follows, we assume that P has dimension d, that is, P is not contained in a proper affine subspace of $\mathbb{R}^d$. Then a polytope $rP = \{r\mathbf{x} \,|\, \mathbf{x} \in P\}$ ($r \in \mathbb{N}$) is called the rth *dilate* of P. (Clearly, if $\mathbf{v}_1, \ldots, \mathbf{v}_k$ are all vertices of P, then rP is the convex hall of $r\mathbf{v}_1, \ldots, r\mathbf{v}_k$.) The number of integer points (that is, points with integer coordinates) in rP is denoted by $L(P,r)$. The following result is due to E. Ehrhart, see [3].

Theorem 1 *$L(P,r)$ is a degree d quasi-polynomial of r whose leading coefficient is equal to the Euclidean volume of P.*

The main tools for the computation of Ehrhart quasi-polynomials are Alexander Barvinok's polynomial time algorithm and its modifications, see [1] and [2].

Let $\mathbf{p} = (p_1, \ldots, p_r)$ be an r-dimensional parameter vector. An *r-dimensional periodic number $U(\mathbf{p})$ on $p_1, \ldots, p_r$* is a function $U : \mathbb{Z}^r \to \mathbb{Q}$ such that there exists $\mathbf{q} = (q_1, \ldots, q_r) \in \mathbb{N}^r$ with the property that $U(p_1, \ldots, p_r) = U(p'_1, \ldots, p'_r)$ whenever $p_i \equiv p'_i (mod\, q_i)$, $1 \leq i \leq r$. The least common multiple of all q_i is called a *period* of U. Say, $[[1, \frac{3}{2}]_{p_2}, [0, \frac{3}{4}]_{p_2}, [-1, \frac{1}{5}]_{p_2}]_{p_1}$ is a 2-periodic number with period 6 ($\mathbf{q} = (3,2)$).

A polynomial in r variables $p_1, \ldots, p_r$, where each coefficient is a multidimensional periodic number on a subset of $\{p_1, \ldots, p_r\}$, is called a *multivariate quasi-polynomial* (in $p_1, \ldots, p_r$). Its *period* is defined as the least common multiple of the periods of the coefficients.

Let $m, n \in \mathbb{N}$, $A \subseteq \mathbb{N}^{m+n}$ and $X_A = \{\mathbf{x} = (x_1, \ldots, x_{m+n}) \,|\, \mathbf{x}$ is not greater than or equal to any $\mathbf{a} \in A$ with respect to the product order $<_P$ on $\mathbb{N}^{m+n}\}$. (Recall that $(a_1, \ldots, a_{m+n}) <_P (x_1, \ldots, x_{m+n})$ if $a_i < x_i$ for $i = 1, \ldots, m+n$.)

Let us fix two sets of positive integers $V = \{v_1, \ldots, v_m\}$ and $W = \{w_1, \ldots, w_n\}$ ("weights") and define the orders of an $(m+n)$-tuple $\mathbf{a} = (a_1, \ldots, a_{m+n}) \in \mathbb{N}$ with

respect to these sets as $\operatorname{ord}_V \mathbf{a} = \sum_{i=1}^{m} v_i a_i$ and $\operatorname{ord}_W \mathbf{a} = \sum_{i=m+1}^{m+n} w_i a_i$, respectively. Furthermore, for any set $A \subseteq \mathbb{N}^{m+n}$ and for any $r, s \in \mathbb{N}$, let

$$A(r,s) = \{\mathbf{a} \in A \mid \operatorname{ord}_V \mathbf{a} \leq r, \operatorname{ord}_W \mathbf{a} \leq s\}.$$

Theorem 2 *With the above notation, there exists a bivariate quasi-polynomial $\phi_{V,W}(t_1,t_2)$ such that*
(i) $\phi_{V,W}(r,s) = \operatorname{Card} X_A(r,s)$ *for all sufficiently large* $(r,s) \in \mathbb{N}^2$. *(It means that there is* $(r_0,s_0) \in \mathbb{N}^2$ *such that the equality holds for all integers* $r \geq r_0$, $s \geq s_0$.*)*
(ii) $\deg_{t_1} \phi_{V,W} \leq m$ *and* $\deg_{t_2} \phi_{V,W} \leq n$.
(iii) $\deg \phi_{V,W} = m+n$ *if and only if* $A = \emptyset$
(iv) $\phi_{V,W}(t_1,t_2) = 0$ *if and only if* $(0,\ldots,0) \in A$.

3. The main result

In what follows we keep the notation of section 1.

Theorem 3 *Let K be a Δ-σ-field and let $L = K\langle \eta_1,\ldots,\eta_q\rangle$ be a Δ-σ-field extension of K generated by a finite set $\eta = \{\eta_1,\ldots,\eta_q\}$. For any $r,s \in \mathbb{N}$, let $L_{r,s} = K(\{\lambda(\eta_i) \mid \lambda \in \Lambda_{V,W}(r,s),\ 1 \leq i \leq q\})$. Then there exists a bivariate quasi-polynomial $\Phi_{\eta|K}^{(V,W)}(t_1,t_2)$ such that*

(i) $\Phi_{\eta|K}^{(V,W)}(r,s) = \operatorname{tr.deg}_K L_{rs}$ *for all sufficiently large* $(r,s) \in \mathbb{N}^2$.

(ii) $\deg_{t_1} \Phi_{\eta|K}^{(V,W)} \leq m = \operatorname{Card} \Delta$ *and* $\deg_{t_2} \Phi_{\eta|K}^{(V,W)} \leq n = \operatorname{Card} \sigma$.

(iii) $\Phi_{\eta|K}^{(V,W)}$ *is an alternating sum of bivariate quasi-polynomials of the form $g(t_1)h(t_2)$ where $g(t_1)$ and $h(t_2)$ are (univariate) Ehrhart quasi-polynomials associated with rational conic polytopes.*

(iv) *The total degree and the coefficient of $t_1^m t_2^n$ of the quasi-polynomial $\Phi_{\eta|K}^{(V,W)}(t_1,t_2)$ are constants that do not depend on the set of difference-differential generators η of the extension L/K.*

This theorem generalizes the result on a bivariate difference-differential dimension polynomial proved in [4]. Furthermore, Theorem 3 allows one to assign a bivariate quasi-polynomial to a system of algebraic difference-differential (Δ-σ-) equations with weighted basic derivations and translations

$$f_i(y_1,\ldots,y_q) = 0 \qquad (i = 1,\ldots,p) \tag{1}$$

($f_i \in R = K\{y_1,\ldots,y_q\}$ $(1 \leq i \leq p)$ where $K\{y_1,\ldots,y_q\}$ denotes the ring of difference-differential polynomials in q variables over K) such that the Δ-σ-ideal P of R generated by the Δ-σ-polynomials $f_1,\ldots,f_p$ is prime (e. g., to a system of linear

difference-differential equations). Systems of this form arise in connection with systems of PDEs with weighted derivatives (see, for example, [7] and [8]) and their finite difference approximations.

In this case, the reflexive closure P^* of the Δ-σ-ideal P is also prime, so one can consider the quotient field of R/P^* as a finitely generated Δ-σ-field extension of K: $L = K\langle \eta_1, \ldots, \eta_q \rangle$ where η_i is the canonical image of y_i in R/P^*. The corresponding bivariate dimension quasi-polynomial $\Phi_{\eta|K}^{(V,W)}(t_1, t_2)$ can be viewed as the Einstein's strength of the system (1) in the sense of the corresponding concepts for systems of partial differential and difference equations (see [6] and [5, Section 7.7] for detail descriptions of these concepts and their expressions as dimension polynomials).

References

[1] A. I. Barvinok, *Computing the Ehrhart polynomial of a convex lattice polytope*, Discrete Comput. Geom. **12**, pp. 35-38 (1994).

[2] A. I. Barvinok and J. E. Pommersheim, *An algorithmic theory of lattice points in polyhedra*, in *New Perspectives in Algebraic Combinatorics*, Math. Sci. Res. Inst. Publ., 38. Cambridge Univ. Press, pp. 91-147 (1999).

[3] E. Ehrhart, *Sur les polyèdres rationnels homothétiques à n dimensions*, C. R. Acad. Sci. Paris, **254**, pp. 616-618 (1962).

[4] A. B. Levin, *Reduced Grobner bases, free difference-differential modules and difference-differential dimension polynomials*, J. Symb. Comput., **29**, pp. 1-26 (2000).

[5] A. B. Levin, *Difference Algebra*. Springer, New York, 2008.

[6] A. V. Mikhalev, E. V. Pankratev, *Differential dimension polynomial of a system of differential equations*, in *Algebra*, Collection of papers. Moscow State Univ., pp. 57-67 (1980).

[7] N. A. Shananin, *On the unique continuation of solutions of differential equations with weighted derivatives*, Sb. Math., **191**, 3-4, pp. 431-458 (2000).

[8] N. A. Shananin, *On the partial quasianalyticity of distribution solutions of weakly nonlinear differential equations with weights assigned to derivatives*, Math. Notes, **68**, 3-4, pp. 519-527 (2000).

Higher-order symmetries and creation operators for linear equations via Maxima and SymPy

M. Janowicz[1], L. Ochnio[2], J. Kaleta[1], A. Zembrzuski[3], and A. Orłowski[3]

[1] *Department of Applied Mathematics, Faculty of Applications of Informatics and Mathematics, Warsaw University of Life Sciences, Poland, maciej_janowicz@sggw.pl*
[2] *Department of Econometrics and Statistics, Faculty of Applications of Informatics and Mathematics, Warsaw University of Life Sciences, Poland,*
[3] *Department of Computer Science, Faculty of Applications of Informatics and Mathematics, Warsaw University of Life Sciences, Poland,*

Computation of symmetries of systems of partial differential equations is one of the oldest applications of computer algebra in the field of differential equations and mathematical physics. Already in the late eighties and early nineties several packages to compute symmetries have been developed in Macsyma, Reduce, Mathematica and Maple[1, 2]. Today, it is actually difficult to imagine *not* to use computer algebra when one faces analysis of complex differential (or difference) system. Skillful application of existent packages leads to efficient analysis of even very complicated systems like those encountered in theory of elasticity, see, e.g., [3].

Let us consider a system of partial differential equations:

$$U = 0, \tag{1}$$

and let X denotes the so-called inifinitesimal generator of symmetries which is a first-order linear partial differential operator. Then there exists the following infinitesimal criterion of symmetry (please see, e.g., [4]):

$$X^{(pr)}U|_{U=0} = 0, \tag{2}$$

where $X^{(pr)}$ is the prolongation of the operators X. The above formula has a simple geometric meaning: the symmetry of Q is such a tranformation (in the space of independent variables, dependent variables, and their derivatives) which leaves the hypersurface of solutions invariant. From the above condition a system of linear partial differential equations can be obtained to compute X. They are called *determining equations*. Even writing down all the determining equations is a very tedious procedure, ideally suited for computers.

In this contribution we, however, take advantage of the fact that for *linear* systems the way to obtain the determining equations is much simpler. Let us restrict ourselves to systems of the form:

$$Q\Psi = 0, \tag{3}$$

where Q is a (variable-coefficient) matrix partial differential operator, and Ψ is a vector of dependent variables. Then, a first-order matrix linear partial differential operator L is called a symmetry operator if and only if [5]:

$$[L,Q] - RQ = 0, \tag{4}$$

where $[,]$ denotes the commutator and R is a function of independent variables.

An important point is that the Eq. (4) can easily be generalized to the higher-order symmetry operators [5]. For instance, in the second-order case we have the following condition:

$$[L^{(2)},Q] - R^{(1)}Q = 0, \tag{5}$$

where $L^{(2)}$ is a second-order, and $R^{(1)}$ - a first-order linear partial differential operators. Unlike the operators L, operators $L^{(2)}$ which satisfy (5) usually do not form a Lie algebra. Computing operators $L, L^{(2)}$ from Eqs. (4, 5) is by far simpler that from (2) but still sufficiently difficult as to require assistance from the computer algebra systems.

We have, in particular, applied both Maxima and SymPy to study the following Schrödinger equation:

$$\left(i\frac{\partial}{\partial t} - H\right)\Psi = 0, \tag{6}$$

where t denotes time and H - a Hamiltonian operator which is given in the representation of second-quantization as:

$$H = \sum_j \alpha_j a_j + \sum_{j,k} \beta_{j,k} a_j^\dagger a_k + \sum_{j,k,l,m} \gamma_{j,k,l,m} a_j^\dagger a_k^\dagger a_l a_m + h.c.,$$

where a_j, $a_k^\dagger$ are the annihilation and creation operators which satisfy:

$$[a_j, a_k^\dagger] = \delta_{jk}, \tag{7}$$

δ_{jk} is the Kronecker delta, “h.c." denotes Hermitian conjugate symbol while α_j, $\beta_{j,k}$, and $\gamma_{j,k,l,m}$ are complex constants. To apply computer algebra, we could, in principle, work directly with the above Hamiltonian using only (7). However, we have found it convenient to use the following Bargmann representation:

$$a_j \to \frac{\partial}{\partial z_j} \quad \text{and} \quad a_k^\dagger \to z_k.$$

In this representation, Ψ becomes a function of time and an analytic function of all z_j.

Using (independently) Maxima and SymPy we have determined the first-, second- and third-order symmetries for a generalized Bose-Hubbard model which describes systems of interacting bosons on a lattice. We also found first- and second-order generalized creation ($A^\dagger$) and annihilation A operators for such model; they have to satisfy the relations:

$$[H,A^\dagger] = A^\dagger \quad and \quad [H,A] = -A.$$

We have found it expedient to work with Maxima and SymPy firstly in the interactive modes, and write the corresponding scripts only later. Regarding Maxima, we observe that its feature which allows to use functions as first-order variables, inherited from Lisp, is a particular advantage. In several cases the symmetries obtained could be used to provide us with separation of variables. In other cases, special interesting exact solutions have been found.

References

[1] Schwarz, F., *Symmetries of Differential Equations: From Sophus Lie to Computer Algbera*, SIAM Rev., **30** (3), pp. 450-481 (1988).

[2] Hereman, W., *Review of symbolic software for Lie symmetry analysis*, in Ibragimov, N.H. (ed) *CRC Handbook of Lie Group Analysis of Differential Equations*, vol. 3 pp. 367-413, CRC Press, Boca Raton (1996).

[3] Michels, D.L., Lyakhov, D.A, Gerdt, V.P., Sobottka, G.A., and Weber, A.G, *Lie Symmetry Analysis of Cosserat Rods*, in Gerdt V.P., Koepf, W., Seiler, W.M., Vorozhtsov E.V (eds.), Computer Algebra in Scientific Computing, Lecture Notes in Computer Science vol. 8660, pp. 324-334 (2014).

[4] Olver, P.J., *Application of Lie groups to differential equations* (Graduate Texts in Mathematics 107), Springer, New York (1986)

[5] Miller W., *Symmetry and separation of variables*, Addison-Wesley, Reading (1977)

Towards a symbolic package for systems of nonlinear difference equations

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*

Difference algebra has been studied in analogy to differential algebra. However, concepts such as characteristic sets for differential systems have not been developed in the same generality for difference systems yet. In particular, methods such as the Rosenfeld-Gröbner algorithm, regular chains and Thomas decomposition for differential systems are not available for difference systems. Among the many applications of difference algebra is, e.g., the consistency analysis of finite difference schemes for partial differential equations.

This talk presents results of trying to transfer the concept of differential Thomas decomposition to systems of nonlinear difference equations and develop a symbolic package for systems of nonlinear difference equations. It reports on joint work with Vladimir Gerdt.

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] F. Boulier, D. Lazard, F. Ollivier and M. Petitot, *Computing representations for radicals of finitely generated differential ideals*, Appl. Algebra Engrg. Comm. Comput. **20**, 1, pp. 73–121 (2009).

[4] R. M. Cohn, *Difference algebra*, John Wiley & Sons, New York, 1965.

[5] X.-S. Gao, Y. Luo and C. M. Yuan, *A characteristic set method for ordinary difference polynomial systems*, J. Symbolic Comput. **44**, 3, pp. 242–260 (2009).

[6] X.-S. Gao, J. van der Hoeven, C. M. Yuan and G. L. Zhang, *Characteristic set method for differential-difference polynomial systems*, J. Symbolic Comput. **44**, 9, pp. 1137–1163 (2009).

[7] V. P. Gerdt, *On decomposition of algebraic PDE systems into simple subsystems*, Acta Appl. Math. **101**, 1-3, pp. 39–51 (2008).

[8] 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).

[9] V. P. Gerdt and R. La Scala, *Noetherian quotients of the algebra of partial difference polynomials and Gröbner bases of symmetric ideals*, J. Algebra **423**, pp. 1233–1261 (2015).

[10] 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`.

[11] 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.

[12] V. P. Gerdt and D. Robertz, *Computation of Difference Gröbner Bases*, Comput. Sci. J. Moldova **20**, 2 (59), pp. 203–226 (2012).

[13] E. R. Kolchin, *Differential algebra and algebraic groups*, vol. 54 of Pure and Applied Mathematics, Academic Press, New York, 1973.

[14] F. Lemaire, M. Moreno Maza and Y. Xie, *The* `RegularChains` *library in MAPLE*, SIGSAM Bull. **39**, pp. 96–97 (2005).

[15] A. Levin, *Difference algebra*, vol. 8 of Algebra and Applications, Springer, New York, 2008.

[16] B. Martin and V. Levandovskyy, *Symbolic Approach to Generation and Analysis of Finite Difference Schemes of Partial Differential Equations*, in: U. Langer and P. Paule (eds.), *Numerical and Symbolic Scientific Computing: Progress and Prospects*, Springer, Vienna, 2012, pp. 123–156.

[17] J. F. Ritt, *Differential Algebra*, vol. XXXIII of American Mathematical Society Colloquium Publications, American Mathematical Society, New York, 1950.

[18] D. Robertz, *Formal Algorithmic Elimination for PDEs*, vol. 2121 of Lecture Notes in Mathematics, Springer, Cham, 2014.

[19] J. M. Thomas, *Differential Systems*, vol. XXI of American Mathematical Society Colloquium Publications, American Mathematical Society, New York, 1937.

Matrices over Differential-difference Algebras

Yang Zhang

University of Manitoba, Winnipeg, Canada, Yang.Zhang@umanitoba.ca

Let R be a ring and σ be a ring endomorphism of R. A σ-derivation on R is a map $\delta : R \longrightarrow R$ satisfying: $\delta(a+b) = \delta(a) + \delta(b)$ and $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$, for all $a, b \in R$. The skew polynomial ring (also called Ore polynomial ring) $R[x;\sigma,\delta]$ over R is the set of usual polynomials in x over R, *i.e.,* $\{\sum r_i x^i \mid r_i \in R\}$, with usual "$+$" and

$$xr = \sigma(r)x + \delta(r), \quad \forall r \in R.$$

We refer to Cohn [1], Goodearl and Warfield [2], Levin[4], and van der Put and Singer[3] for more details and the related topics.

Matrices over skew polynomial rings (also called Ore matrices) have been studied for decades with many applications in other areas like control theory and engineering. In this talk, we focus on various generalized inverses of Ore matrices.

Let K be a ring with an involution "$*$". For $A \in K^{m\times n}$ and $X \in K^{n\times m}$, consider the following equations:

$$(i)\ AXA = A,\ \ (ii)\ XAX = X,\ \ (iii)\ (AX)^* = AX,\ \ (iv)\ (XA)^* = XA,$$

where A^* is the transpose conjugate of A. If a matrix $X \in K^{n\times m}$ satisfies (i), then X is called a $\{1\}$-inverse of A. A matrix $X \in K^{n\times m}$ satisfying both of (i) and (ii) is called a $\{1,2\}$-inverse of A, and so on. In particular, X satisfying $\{i, ii, iii, iv\}$ is called the Moore-Penrose inverse of A, denoted by $A^\dagger$. More generalized inverses of matrices like group inverses and Drazin inverses of matrices can be found in [5].

We first use Jacobson forms of Ore matrices to discuss $\{1\}$-inverses. One of theorems is as follows:

Theorem. For any $A \in R[x;\sigma,\delta]^{m\times n}$, A has a $\{1\}$-inverse over $R[x;\sigma,\delta]$ if and only if its Jacobson form equals $\begin{bmatrix} I_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$, that is, there exist invertible matrices $P \in R[x;\sigma,\delta]^{m\times m}$ and $Q \in R[x;\sigma,\delta]^{n\times n}$ such that $A = P \begin{bmatrix} I_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} Q$. Furthermore, if X is a $\{1\}$-inverse of A over $R[x;\sigma,\delta]$, then X can be written as $Q^{-1}\begin{bmatrix} I_r & W_2 \\ W_3 & W_4 \end{bmatrix} P^{-1}$, where W_2, W_3, W_4 are arbitrary matrices over $R[x;\sigma,\delta]$.

As applications of $\{1\}$-inverses, we discuss Roth theorems and generalized Sylvester matrix equation, for example,

Theorem. If Ore matrices A, B, C and D all have $\{1\}$-inverses over $R[x;\sigma,\delta]$, then the following statements are equivalent:

1. The matrix equation $AXB+CYD=E$ has solutions over $R[x;\sigma,\delta]$.
2. The matrix equations $AX_1+Y_1D=E$ and $X_2B+CY_2=E$ have solutions over $R[x;\sigma,\delta]$.
3. $\text{rank}\begin{pmatrix} C & E & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & B & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & A & E \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & D \end{pmatrix} = \text{rank}\begin{pmatrix} C & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & B & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & A & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & D \end{pmatrix}$ over $R[x;\sigma,\delta]$.
4. The matrix equation $\begin{bmatrix} C & \mathbf{0} \\ \mathbf{0} & A \end{bmatrix} X_3 + Y_3 \begin{bmatrix} B & \mathbf{0} \\ \mathbf{0} & D \end{bmatrix} = \begin{bmatrix} E & \mathbf{0} \\ \mathbf{0} & E \end{bmatrix}$ has solutions over $R[x;\sigma,\delta]$.

For Moore-Penrose inverses, assume that R is a division ring with an involution "$*$". We give the sufficient and necessary conditions for extending "$*$" to be an involution on $R[x;\sigma,\delta]$, and then prove the following theorems:

Theorem. For any $A \in R[x;\sigma,\delta]^{m\times n}$, $A^\dagger$ exists over $R[x;\sigma,\delta]$ if and only if A^*AA^* has a $\{1\}$-inverse over $R[x;\sigma,\delta]$, and $\text{rank}(A) = \text{rank}(AA^*) = \text{rank}(A^*A)$. Moreover $X = A^*(A^*AA^*)^{(1)}A^*$ is the unique MP-inverse of A over $R[x;\sigma,\delta]$.

Theorem. For any $A \in R[x;\sigma,\delta]^{m\times n}$, if the Jacobson form of A is $\begin{bmatrix} I_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$, i.e., there exist invertible matrices $P \in R[x;\sigma,\delta]^{m\times m}$ and $Q \in R[x;\sigma,\delta]^{n\times n}$ such that $A = P\begin{bmatrix} I_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} Q$, where $P = \begin{bmatrix} P_1 & P_2 \end{bmatrix}$, $Q = \begin{bmatrix} Q_1 \\ Q_2 \end{bmatrix}$, $P_1 \in R[x;\sigma,\delta]^{m\times r}$ is the first r columns of P and $Q_1 \in R[x;\sigma,\delta]^{r\times n}$ is the first r rows of Q, then $A^\dagger$ exists over $R[x;\sigma,\delta]$ if and only if the Jacobson form of $P_1^*P_1Q_1Q_1^*$ is I_r.

As applications, we give the general solutions for the linear systems of differential-difference polynomials, and some types of matrix equations.

This is a joined work with Qiwei Feng.

References

[1] P. M. Cohn, *Free ideal rings and localization in general rings*, Cambridge University Press, 2006.

[2] K. R. Goodearl and R. B. Warfield, Jr, *An introduction to noncommutative noetherian rings, second edition*, Cambridge University Press, 2004.

[3] M. van der Put and M.F. Singer, *Galois Theory of Linear Differential Equations*, Grundlehren der mathematischen Wissenschaften, Volume 328, Springer, 2003.

[4] A. B. Levin, *Difference Algebra*, Springer, 2008.

[5] Adi Ben-Israel and Thomas N.E. Greville, *Generalized Inverses: Theory and Applications*, Springer, 2003.

Session 4

Computer algebra modeling in science and engineering

Session chairs:

Alexander Prokopenya
Faculty of Applied Informatics and Mathematics, Warsaw University of Life Sciences - SGGW, Poland

Haiduke Sarafian
Professor of Physics and Endowed Chair of John T. and Paige S. Smith Professor of Science, The Pennsylvania State University, USA

Finite Fields, Computer Algebra Systems, and Non-Linear Coding

S. Engelberg[1], O. Keren[2]

[1] *Department of Electrical and Electronics Engineering, School of Engineering and Computer Science, Jerusalem College of Technology, Jerusalem, Israel, shlomoe@jct.ac.il*

[2] *School of Engineering, Bar-Ilan University, Ramat-Gan, Israel, Osnat.Keren@biu.ac.il*

We consider linear and non-linear codes. We start by developing a conservation law for codes. We then explain why linear codes, which are easy to understand and implement, are useful when one is interested in protecting data from rarely occuring random errors. By a simple argument, we demonstrate that linear codes are not a good way to protect data from an attacker. Having ruled out linear codes for this purpose, we take up non-linear codes. We explain what a finite field is and how data can be represented by elements of a finite field. We then consider codes that are non-linear functions of the data – of the elements of the finite field. We show that quadratic codes suffer from the same drawbacks as linear codes. Next we consider cubic codes. First we show that if all that one is concerned with are attackers, cubic codes are optimal. Many of the above results are due to M. Karpovsky and his co-workers. (See, for example, [2].)

Then we show how by making use of a computer algebra system we were able to formulate a conjecture that certain cubic codes provide optimal protection against attackers and some protection against certain relatively common random errors. We will then sketch the proof of this result and describe some extensions of the result [1].

References

[1] S. Engelberg and O. Keren, "A Comment on the Karpovsky-Taubin Code," *IEEE Trans. Inf. Theory*, Vol. 57, No. 12 (2011).

[2] M. G. Karpovsky and A. Taubin, "A new class of nonlinear systematic error detecting codes," *IEEE Trans. Inf. Theory*, Vol. 50, No. 8 (2004).

A Modified Hermite Interpolation with Exponential Parameterization

R. Kozera[1,2] and M. Wilkołazka[3]

[1] *Warsaw University of Life Sciences - SGGW, Poland, ryszard.kozera@gmail.com*
[2] *The University of Western Australia, Perth, Australia,ryszard.kozera@csse.uwa.edu.au*
[3] *The John Paul II Catholic University of Lublin, Lublin, Poland,magdalena.wilkolazka@gmail.com*

This work addresses the problem of estimating the unknown trajectory of a regular curve $\gamma : [0,T] \to E^n$ based on the so-called *reduced data* Q_m. The latter represent $m+1$ ordered interpolation points $Q_m = \{q_i\}_{i=0}^m$ (with $q_{i+1} \neq q_i$) in arbitrary Euclidean space E^n subject to the constraint $q_i = \gamma(t_i)$. We assume that the respective knots $\mathscr{T}_m = \{t_i\}_{i=0}^m$ satisfying $t_i < t_{i+1}$ are not given. In order to fit Q_m with the prescribed interpolation scheme, one also needs to substitute somehow the unknown knots $\mathscr{T}_m$ with another family of parameters $\hat{\mathscr{T}}_m = \{\hat{t}_i\}_{i=0}^m$ satisfying $\hat{t}_i < \hat{t}_{i+1}$. In doing so, the so-called *exponential parameterization* depending on a single parameter $\lambda \in [0,1]$ and Q_m can e.g. be used. This ultimately yields $\hat{\mathscr{T}}_m^{\lambda} = \{\hat{t}_i^{\lambda}\}_{i=0}^m \approx \mathscr{T}_m$ - see e.g. Refs. [1, 2]. Note that a special case of $\lambda = 1$ introduces the so-called *cumulative chord parameterization* of reduced data Q_m (see e.g. Ref. [1]). In the next step a classical *Hermite interpolation* (see Ref. [3]) $\hat{\gamma}_H : [0,\hat{T}] \to E^n$ based on Q_m and $\hat{\mathscr{T}}_m^{\lambda}$ can be invoked (with $\hat{T} = \hat{t}_m^{\lambda}$). However, the respective missing velocities $\{v_i = \dot{\gamma}(t_i)\}_{i=0}^m$ along Q_m are approximated here according to $\hat{v}_i = \hat{\gamma}_{3,i}'(\hat{t}_i^{\lambda})$, where $\hat{\gamma}_{3,i} : [\hat{t}_i^{\lambda}, \hat{t}_{i+3}^{\lambda}] \to E^n$ denotes a standard Lagrange cubic satisfying $\hat{\gamma}_{3,i}(\hat{t}_{i+j}) = q_{i+j}$ (for $j = 0,1,2,3$) - see Ref. [3]. Note that here we apply in fact "overlapped" Lagrange cubics to estimate all velocities $\{v_i\}_{i=0}^m$ at $\{Q_m\}_{i=0}^m$. More precisely, for $\hat{\gamma}_{3,i+1} : [\hat{t}_{i+1}^{\lambda}, \hat{t}_{i+4}^{\lambda}]$ interpolating $\{q_{i+1+j}\}_{j=0}^3$ we adopt a similar estimate i.e. $\hat{v}_{i+1} = \hat{\gamma}_{3,i+1}'(\hat{t}_{i+1}^{\lambda})$ of $\dot{\gamma}(t_{i+1})$. For the last four interpolation points $\{q_i\}_{i=m-3}^m$ the above procedure can be repeated upon changing the order of points and taking the computed derivatives with the opposite sign. Such construction of $\hat{\gamma}_H$ based on $\hat{\mathscr{T}}_m^{\lambda}$, $\{\hat{v}_i\}_{i=0}^m$ and Q_m is coined *a modified Hermite interpolation*. A special case when $\lambda = 1$ is discussed in more details in Refs. [4, 5].

Given $\delta_m = \max_{0 \leq i \leq m-1}\{t_{i+1} - t_i\}$ the sampling $\mathscr{T}_m$ is called *admissible* if $\lim_{m\to\infty} \delta_m = 0$. The subfamily of admissible samplings is called *more-or-less uniform* if there exists $\beta \in (0,1]$ such that $\delta_m \beta \leq t_{i+1} - t_i$, holding for all $i = 0,1,\ldots,m-1$ and arbitrary m. The question of approximating γ by modified Hermite interpolant $\hat{\gamma}_H$ is studied merely for the special case of $\lambda = 1$ i.e. for cumulative chord parameterization in Refs. [4, 5]. More specifically, quratic order of convergence in trajectory approximation is proved and confirmed numerically in the above last cited papers. We extend this result to the remaining $\lambda \in [0,1)$

determining the exponential parameterization. Indeed the following holds:

Theorem 1 *Assume that a regular $\gamma : [0,T] \to E^n$ of class C^4 with the unknown interpolation knots $\{t_i\}_{i=1}^m$ is sampled more-or-less uniformly. If $\hat{\gamma}_H$ represents a modified Hermite interpolant based on reduced data Q_m and exponential parameterization governed by $\lambda \in [0,1]$, then for some piecewise-cubic-C^∞ $\psi : [0,T] \to [0,\hat{T}]$:*

$$(\hat{\gamma}_H \circ \psi)(t) = \gamma(t) + O(\delta_m^1) \text{ for } \lambda \in [0,1) \text{ and } (\hat{\gamma}_H \circ \psi)(t) = \gamma(t) + O(\delta_m^4) \text{ for } \lambda = 1. \quad (1)$$

Theorem 1 establishes a substantial deceleration in convergence rates for trajectory estimation (to the linear one) while λ runs over $[0,1)$. The latter contrasts with the fast quartic order holding for $\lambda = 1$ as specified in (1) (see also Ref. [4]). The numerical tests conducted in this work (with the aid of *Mathematica* package - see Ref. [7]) confirm the sharpness of the estimates from (1). A similar effect of the left-hand side discontinuity in convergence rate at $\lambda = 1$ is proved for piecewise-quadratic Lagrange intepolation based on exponential parameterization and Q_m - see Refs. [2, 6]. Fitting reduced data is an important problem in computer vision and graphics, as well as in engineering, microbiology, physics and other applications like medical image processing - see e.g. [1].

References

[1] B.I. Kvasov, *Methods of Shape-Preserving Spline Approximation*, World Scientific Publishing Company, Singapore (2000).

[2] R. Kozera and L. Noakes, *Piecewise-quadratics and exponential parameterization for reduced data*, Applied Mathematics and Computation **221**, pp. 1–19 (2013).

[3] C. de Boor, *A Practical Guide to Spline*, Springer-Verlag, New York Heidelberg Berlin (1985).

[4] R. Kozera and L. Noakes, *C^1 interpolation with cumulative chord cubics*, Fundamenta Informaticae **61**, 3-4, pp. 285–301 (2004).

[5] R. Kozera, *Curve modeling via interpolation based on multidimensional reduced data*, Studia Informatica **25**, 4B(61), pp. 1–140 (2004).

[6] R. Kozera and L. Noakes, *Piecewise-quadratics and ε-uniformly sampled reduced data*, Applied Mathematics and Information Sciences **10**, 1, pp. 33–48 (2016).

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

Interval Nonlinear Solver with Symbolic Preprocessing for Training AI Tools in Presence of Perturbations

Bartłomiej Jacek Kubica[1], Jarosław Kurek[2]

[1] *Department of Applied Informatics, Warsaw University of Life Sciences, Poland, bartlomiej_kubica@sggw.pl*
[2] *Department of Applied Informatics, Warsaw University of Life Sciences, Poland, jaroslaw_kurek@sggw.pl*

Training various artificial intelligence (AI) tools is a hard problem, often requiring to solve a difficult nonlinear optimization problem. Numerical finding its solution can be significantly accelerated by proper symbolic techniques.

This is the case as for artificial neural networks (ANN); e.g., [8], as for support vector machines (SVM); e.g., [10], and for many other techniques.

To be succinct, we can either solve the optimization problem:

$$\min_w \sum_i ||f(x_i, w) - y_i|| \ , \tag{1}$$

or the nonlinear system:

$$f(x_i, w) - y_i = 0 \ \text{ for all } i = 1, \ldots, N \ . \tag{2}$$

In the above formulae, (x_i, y_i) are training examples and w is the vector of parameters, we are trying to determine in the learning process. For an ANN w represents weights of links between neurons; for SVM – parameters of the Gaussian kernel and of the soft margin.

To train the AI tools we can, in particular, solve the system of nonlinear equations, representing the necessary conditions for optimality of (1) or solve the system (2) directly. Other equations systems also arise in training such tools (e.g., [3]).

Solutions of such systems can be found by a few algorithms. We propose using interval methods (see, e.g., [5]), as this approach has proven to be useful in solving nonlinear systems – both well-determined and underdetermined ones.

One of the advantages of interval calculus is that it can deal with uncertainties in data, in a natural manner: instead of taking specific numbers (x_i, y_i) as inputs, we can use intervals $(\boldsymbol{x}_i, \boldsymbol{y}_i)$, containing the perturbed values.

The solver we use for training all these tools is HIBA_USNE [4], described, i.a., in [6], [7]. Interval arithmetic is augmented by the use of algorithmic differentiation [1] and symbolic preprocessing techniques, based on CoCoALib [2] to improve the performance of the interval solver. For an ANN, the systems of equations are non-polynomial, but it can still benefit from some symbolic techniques. As we encounter terms of the form $\exp\left(\sum_{i=1}^{N} w_i x_i\right)$, we can add new terms $t_i = \exp(w_i x_i)$. In case the terms repeat in other equations, they can be removed using the Gröbner basis theory. The paper is going to discuss possible improvements, obtained by this approach.

As an illustrative example, we consider the problem of determining the state of a drill (good, suspicious, damaged). We apply ANNs and SVMs to solve it.

In the paper we are going to present computational results for both AI tools. We show how interval methods combined with computer algebra and algorithmic differentiation help to model perturbations and tune the classifiers in their presence.

References

[1] *ADHC*, Algorithmic Differentiation and Hull Consistency enforcing, C++ library, `https://www.researchgate.net/publication/316687827_HIBA_USNE_Heuristical_Interval_Branch-and-prune_Algorithm_for_Underdetermined_and_well-determined_Systems_of_Nonlinear_Equations_-_Beta_25` (2017).

[2] J. Abbott and A. M. Bigatti, *CoCoALib: a C++ library for doing Computations in Commutative Algebra*, `http://cocoa.dima.unige.it/cocoalib` (2017).

[3] M. Beheshti and A. Berrached and A. de Korvin and C. Hu and O. Sirisaengtaksin, *On interval weighted three-layer neural networks*, in *Proceedings of Simulation Symposium*, IEEE, pp. 188-194 (1998).

[4] *HIBA_USNE*, Heuristical Interval Branch-and-prune Algorithm for Underdetermined and well-determined Systems of Nonlinear Equations, C++ library, `https://www.researchgate.net/publication/316687827_HIBA_USNE_Heuristical_Interval_Branch-and-prune_Algorithm_for_Underdetermined_and_well-determined_Systems_of_Nonlinear_Equations_-_Beta_25` (2017).

[5] R. B. Kearfott, *Rigorous Global Search: Continuous Problems*, Kluwer, Dordrecht, 1996.

[6] B.J. Kubica, *Presentation of a highly tuned multithreaded interval solver for underdetermined and well-determined nonlinear systems*, Numerical Algorithms, **70**, 4, pp. 929–963 (2015).

[7] B.J. Kubica, *Parallelization of a bound-consistency enforcing procedure and its application in solving nonlinear systems*, Journal of Parallel and Distributed Computing, published online `https://doi.org/10.1016/j.jpdc.2017.03.009` (2017).

[8] J. Kurek and S. Osowski, *Support vector machine for fault diagnosis of the broken rotor bars of squirrel-cage induction motor*, Neural Computing and Applications, **19**, 4, pp. 557-564 (2010).

[9] *LIBSVM* C++ library, `https://www.csie.ntu.edu.tw/~cjlin/libsvm/` (2017).

[10] B. Świderski and J. Kurek and S. Osowski, *Multistage classification by using logistic regression and neural networks for assessment of financial condition of company*, Decision Support Systems, **52**, 2, pp. 539-547 (2012).

Modelling Atwood's Machine with Three Degrees of Freedom

Alexander N. Prokopenya

Warsaw University of Life Sciences – SGGW, Warsaw, Poland,
alexander_prokopenya@sggw.pl

An Atwood machine is a well-known device that consists of two bodies of different masses m_1, m_2 attached to opposite ends of a massless inextensible thread wound round a massless frictionless pulley (see Ref. [1]). 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 that is usually used in the course of physics for demonstration of the uniformly accelerated motion of the system.

However, it is very difficult in practice to attain such a simple translational motion and the oscillations of the bodies inevitably arise. These oscillations may modify the system motion significantly and so the swinging Atwood machine has been a subject of a number of papers (see, for example, Refs. [2, 3, 4, 5, 6]). 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.

To clarify the physical reasons of such influence of oscillation on the system motion in the previous paper [7] we considered the simplest generalization of the Atwood machine when only one body of mass m_1 is allowed to swing in a plane while the other body of mass $m_2 > m_1$ can move only along a vertical. We have shown that oscillation results in increasing of the averaged thread tension which depends on the amplitude of oscillation. If increase of the averaged tension exceeds $(m_2 - m_1)g$, where g is a gravity acceleration, the body of smaller mass m_1 can pull the body m_2 up what is not possible in the system without oscillation.

In the present paper we consider the more complicated Atwood machine when both bodies are allowed to swing in the plane. Such a system has three degrees of freedom and can demonstrate different kinds of quasi-periodic motion depending on the masses difference and initial conditions. However, the equations of motion become more complicated and their analysis requires to combine symbolic and numerical calculations. We demonstrate here that such analysis can be successfully done with the computer algebra system Mathematica (see Ref. [8]) that is used for doing all relevant calculations and visualization of results.

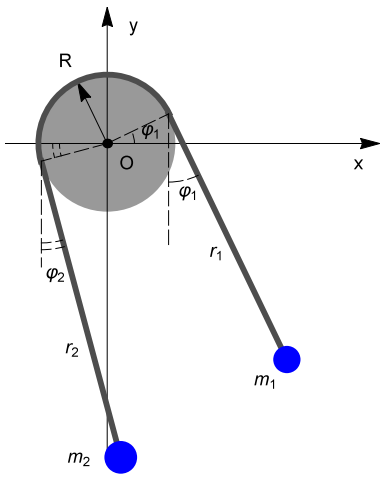


Figure 1: Atwood's machine with three degrees of freedom.

1 Equations of Motion

We consider a generalized model of the simple Atwood machine when both bodies are allowed to swing in the plane (see Fig. 1). Such a system has three degrees of freedom and its geometrical configuration can be described in terms of three variables, for example, two angles φ_1 and φ_2 determining deviations of the thread from the vertical and a length r of the thread between the body m_1 and the point, where the thread departs from the pulley in case of $\varphi_1 = 0$. Note that a length of the thread between the body m_2 and the point, where the thread departs from the pulley, is given by $(L - \pi R - r - R\varphi_2)$, where L is the length of the thread and R is a radius of the pulley.

The Lagrangian of the system can be written in the form

$$\begin{aligned}\mathscr{L} = \frac{(m_1+m_2)R^2+I_0}{2R^2}\dot{r}^2 + \frac{m_1}{2}\left(r+R\varphi_1\right)^2\dot{\varphi}_1^2 \\ +\frac{m_2}{2}\left(L-r-\pi R-R\varphi_2\right)^2\dot{\varphi}_2^2 - m_1 g\left(R\sin\varphi_1-(r+R\varphi_1)\cos\varphi_1\right) \\ +m_2 g\left(R\sin\varphi_2+(L-r-\pi R-R\varphi_2)\cos\varphi_2\right)\ , \qquad (1)\end{aligned}$$

where the dot denotes differentiation with respect to time, and I_0 is a moment of inertia of the pulley. Using Eq. (1) and doing standard symbolic calculations, we obtain the equations of motion in the form

$$\kappa\ddot{r} = g(\cos\varphi_1 - \mu\cos\varphi_2) + (r+R\varphi_1)\dot{\varphi}_1^2 - \mu(L-r-\pi R-R\varphi_2)\dot{\varphi}_2^2\ , \qquad (2)$$

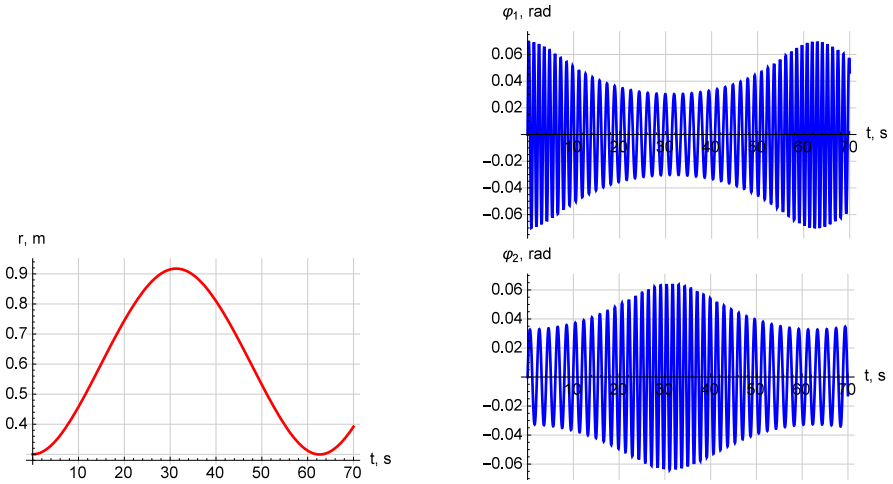


Figure 2: Motion of the Atwood machine in case of $m_1 = m_2$.

$$(r + R\varphi_1)\ddot{\varphi}_1 = -g\sin\varphi_1 - 2\dot{r}\dot{\varphi}_1 - R\dot{\varphi}_1^2 \,, \tag{3}$$

$$(L - r - \pi R - R\varphi_2)\ddot{\varphi}_2 = -g\sin\varphi_2 + 2\dot{r}\dot{\varphi}_2 + R\dot{\varphi}_2^2 \,, \tag{4}$$

where $\mu = m_2/m_1$,

$$\kappa = \frac{I_0 + (m_1 + m_2)R^2}{m_1 R^2} \,.$$

2 Main result

One can readily check that equations of motion (2)-(4) cannot be solved symbolically. However, choosing some realistic values of the system parameters, we can obtain the corresponding numerical solution for different initial conditions and analyze motion of the system.

As an example, let us consider the case of equal masses ($m_1 = m_2$) and assume that the bodies are at rest. If the body of mass m_1 gets a small horizontal initial velocity it starts to oscillate. As a result an average value of the thread tension becomes greater than the gravity force $m_2 g$ and the oscillating body starts to move down and pull up the second body (see [7]). However, if both bodies being at rest get different horizontal initial velocities then both of them start to oscillate with different amplitudes. Solving Eqs. (2)-(4) with the initial conditions $\varphi_1(0) = \varphi_2(0) = \dot{r}(0) = 0$, $r(0) = 0.3$, $\dot{\varphi}_1(0) = 0.4$, $\dot{\varphi}_2(0) = 0.1$, for instance, we obtain a solution shown in Fig. 2.

One can readily see that initially the body of mass m_1 oscillates with the amplitude being greater than that of the body m_2. Consequently, the thread tension in the right-hand side of the system is greater than in the left-hand side and the body m_1 moves down and pull up the body m_2. However, a length of the thread between the body m_1 and the pulley increases and amplitude of its oscillation decreases while amplitude of the body m_2 oscillation grows up. Finally, an average tension of the thread between the body m_2 and the pulley becomes greater that the tension in the right-hand side of the system. As a results the pulley stops and then starts to rotate in opposite direction. Then the roles of the bodies change and the system continues its motion. Thus, due to oscillations of the bodies the system demonstrates quasi-periodic motion which is not possible in case of the classical Atwood machine with bodies of equal masses.

3 Conclusions

In the present talk we have demonstrated an influence of oscillation on the Atwood machine motion in the case when both bodies are allowed to oscillate in a plane. Simulating motion of such Atwood's machine with the computer algebra system Wolfram Mathematica, we have shown that even small oscillations can completely modify its motion, while the simple Atwood machine demonstrates only the uniformly accelerated motion of the bodies. Note that such simulation 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] A.N. Prokopenya, *Motion of a swinging Atwood's machine: simulation and analysis with Mathematica*, Math. Comput.Sci. (2017) doi: 10.1007/s11786-017-0301-9.

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

Two Dimensional Dipole-Dipole Interaction and Generalized Orbitals Under the Influence of Noncentral Forces

Haiduke Sarafian

The Penssylvania State Uninversity, York, PA, USA, has2@psu.edu

In this investigation with two objectives we augment the scope of our previous analyses addressing the impact of two mutually interactive magnetic dipoles. First we deviate from restricting the movement of one of the loose magnets to one dimension; this is addressed in [1]. In this scenario the interactive force is a distance dependent function only. The resulting equation of motion is a nonlinear differential equation. Utilizing a computer algebra system, Mathematica [2] numeric solution of the equation of motion including viscosity is proven in agreement with data. Second, we apply our theory analyzing the orbitals of a loose particle under the influence of a hypothetical noncentral force [3,4,5]. Because of the noncentrality of the force the resulting equations of motion are coupled ODEs. Applying Mathematica and utilizing the numeric solutions deducing the orbits. In this current analysis by adopting the same strategy we utilize a realistic format for the mutual interaction force between two planar magnetic dipoles [6]. In this scenario one of the magnets is kept in place and the second one is mobile. The force is realistic, its format coincides with the fifteenth class of the forces reported in [5], namely, $f_{44}(r,\theta)\hat{r}+g_{44}(r,\theta)\hat{\theta}$, Table 1. Here depending to the orientation of two planar magnets we consider four different scenarios. For each situation we solve the associated coupled nonlinear differential equation of motions numerically; Mathematica provides the solutions. Utilizing the solutions we deduce the kinematics of the mobile magnet displaying the orbitals. We provide also an interactive Mathematica simulation program addressing the potential "what if" scenarios.

References

[1] Haiduke Sarafian, " Dynamic Dipole-Dipole Magnetic Interaction and Damped Nonlinear Oscillations", Journal of Electromagnetic Analysis & Applications, 2009, 1: 195-204 doi:10.4236/jemaa.2009.14030 Published Online December 2009 (http://www.SciRP.org/journal/jemaa).

[2] Stephen Wolfram, *Mathematica* "A general computer software system and language intended for mathematical and other applications",V11.0, Wolfram Research, 2016.

[3] Haiduke Sarafian, Masataka Kaneko and Setsuo Takato, "Central Conservative Forces and Orbits Beyond Conic Sections," Difference Equations Conference, Abstract Book, 58, Izmir University of Economics, Turkey, 2014.

[4] Haiduke Sarafian, Takato, S., and Kaneko, M. (2014) "Central Conservative Forces and Orbits beyond Conic Sections." The Journal of Mathematics and System Sciences, 4, 579-585. www.davidpublishing.org/journals_info.asp?jId=2039.

[5] Haiduke Sarafian, "Generalized Orbitals Under The Influence of 2D Central and Noncentral Forces", World Journal of Mechanics, 2014, 4, 303-308,Published Online October 2014 in SciRes. http://www.scirp.org/journal/wjm, http://dx.doi.org/10.4236/wjm.2014.410030.

[6] Kar W. Yung, Peter B. Landecker and Daniel D. Villani, "An Analytic Solution For The Force Between Two Magnetic Dipoles," Magnetic and Electrical Separation, Vol. 9, pp. 39-52, 1998, Overseas Publishers Association, N.V.

New Gronwall Type Inequality For the Caputo Fractional Differential Operator and Applications

Weiwei Sun

Department of Mathematics, City University of Hong Kong
maweiw@math.cityu.edu.hk

Time-fractional differential equations have been attractive in the past decades since many natural phenomena in physics, biology and chemistry can be described more precisely in this way. Numerous effort has been devoted in developing effective methods for time-fractional differential equations and simulations on a large range of physical problems. However, numerical analysis for time-fractional differential equations has not been well done, mainly due to the lack of a fundamental Gronwall type inequality. Such an inequality for first-order derivative and its approximations services as an essential tool in analysis of ODEs and PDEs. In this talk, we shall present our recent work in establishing a new fundamental algebraic Gronwall type inequality for several approximations to the Caputo fractional derivative, in terms of Mittag-Leffler function. Matlab software has also been used to verify our formulations. With the proved Gronwall type inequality, we provide theoretical analysis for several discrete algebraic methods. The theoretical results are illustrated by applying our proposed methods to three examples: linear Fokker-Planck equation, nonlinear Huxley equation and Fisher equation.

Syzygies for Translational Surfaces

H. Wang[1], R. Goldman[2]

[1] *Southeast Missouri State University, U.S.A., hwang@semo.edu*
[2] *Rice University, U.S.A rng@rice.edu*

A translational surface is a rational tensor product surface generated from two rational space curves by translating either one of these curves parallel to itself in such a way that each of its points describes a curve that is a translation along the other curve. Translational surfaces, ruled surfaces, swept surfaces, along with low degree surfaces such as quadratic and cubic surfaces, are basic modeling surfaces that are widely used in computer aided geometric design and geometric modeling.

Since translational surfaces are generated from two space curves, translational surfaces have simple representations. The simplest and perhaps the most common representation of a translational surface is given by the rational parametric representation $\mathbf{h}^*(s;t) = \mathbf{f}^*(s) + \mathbf{g}^*(t)$, where $\mathbf{f}^*(s)$ and $\mathbf{g}^*(t)$ are two rational space curves. Translational surfaces represented by $\mathbf{h}^*(s;t) = \mathbf{f}^*(s) + \mathbf{g}^*(t)$ have been investigated by differential geometers, and also studied from a geometric modeling point of view.

Translational surfaces defined by $\mathbf{h}^*(s;t) = \mathbf{f}^*(s) + \mathbf{g}^*(t)$ are not translation invariant: translating both curves $\mathbf{f}^*$ and $\mathbf{g}^*$ by the vector $\mathbf{v}$ translates the surface $\mathbf{h}^*$ by the vector $2\mathbf{v}$. One would like to define translational surfaces in such a way that translating the two generating curves by the same vector $\mathbf{v}$, also translates every point on the surface by the vector $\mathbf{v}$. In this presentation, we offer an alternative definition of translational surfaces given by the rational parametric representation $\mathbf{h}^*(s;t) = \frac{\mathbf{f}^*(s)+\mathbf{g}^*(t)}{2}$, where $\mathbf{f}^*(s)$ and $\mathbf{g}^*(t)$ are two rational space curves. Under this definition, these translational surfaces consist of all the midpoints of all the lines joining a point on $\mathbf{f}^*$ to a point on $\mathbf{g}^*$, so these translational surfaces are invariant under rigid motions: translating and rotating the two generating curves translates and rotates these translational surfaces by the same amount. Hence, applying a rigid motion to a translational surface can be achieved by applying the same rigid motion to the two rational space curves that generate the surface. Therefore, one can control these translational surfaces simply by manipulating the generating curves.

In this presentation, we will investigate the translational surfaces given by the rational parametric representation $\mathbf{h}^*(s;t) = \frac{\mathbf{f}^*(s)+\mathbf{g}^*(t)}{2}$. Our main goal is to utilize syzygies to study translational surfaces. We will construct three special syzygies for a translational surface from the μ-basis of one of the generating space curves. In addition, we will examine many properties of translational surfaces, and compute the implicit equation and singularities from these three special syzygies.

The outline of the presentation is structured as the following. First, we introduce the definition of translational surfaces, provide a few examples of translational surfaces generated from two rational space curves, and investigate a few special characteristics of translational surfaces. Second, we study syzygies of translational surfaces, relate the syzygies of the generating curves to the syzygies of the corresponding translational surface, and compute the implicit equation of a translational surface from the resultant of the three moving planes. Third, we focus on ruled translational surfaces and compute their implicit equations based solely on the μ-bases of the generating curves. Fourth, we detect the self-intersections of translational surfaces. Finally, we observe that the techniques used in this paper can be applied with only minor modifications to the translational surfaces defined by $\mathbf{h}^*(s;t) = a\mathbf{f}^*(s) + b\mathbf{g}^*(t)$, where a, b are real numbers and $ab \neq 0$. In the case of $a = b = 1$, we provide a necessary and sufficient condition for a rational tensor product surface to be a translational surface.

Systems of polynomial equations arise throughout mathematics, science, and engineering. Algebraic geometry provides powerful theoretical techniques for studying the qualitative and quantitative features of their solution sets. This talk presents algorithmic tools for algebraic geometry and experimental applications, as well as introduces software systems in which the tools have been implemented and with which the experiments can be carried out. Computer algebra system such as Singular [1], Macaulay 2 [2], Maple [3], and Mathematica [4] are used to compute examples and generate graphics.

For instance, consider the translational surface given by

$$\mathbf{h}^*(s;t) = \frac{(s^2-1, s(s^2-1), 0)}{2} + \frac{(t, 0, -t^2)}{2} = \frac{\mathbf{f}^*(s) + \mathbf{g}^*(t)}{2}. \qquad (1)$$

Figure 1 generated by Mathematica [4] is an affine view of the surface $\mathbf{h}^*(s;t)$ given in Equation (1), where the highlighted curves are the curves $\mathbf{f}^*(s)$ and $\mathbf{g}^*(t)$.

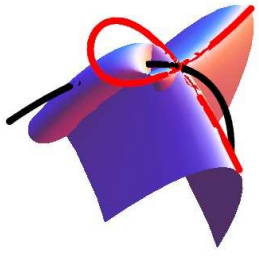


Figure 1: Surface $\mathbf{h}^*(s;t) = \frac{(t+(s^2-1), s(s^2-1), -t^2)}{2}$

The translational surface given by Equation (1) has a base point. The search

for techniques for implicitizing rational surfaces with base points is a very active area of research because base points show up quite frequently in practical industrial design. It is often difficult to compute the multiplicity of base points, and to implicitize a surface that has a complicated collection of base points. Singular [1] and Macaulay 2 [2] have computer algebra packages aimed at algebraic geometry and commutative algebra to compute the multiplicity of the base points. The implicit equation of the surface $\mathbf{h}^*(s;t)$ in Equation (2) is computed from the resultant of three moving planes. Maple [3], Singular [1], and Macaulay 2 [2] have implemented packages to compute multivariate resultant. We carried out our computation via Macaulay 2 [2].

$$\begin{aligned} F(x,y,z) &= 4x^4+16x^5+16x^6-8x^2y^2-16x^3y^2+4y^4+4x^2z+16x^3z \\ &\quad +24x^4z+4y^2z+24xy^2z+z^2+4xz^2+12x^2z^2+2z^3 \qquad (2) \\ &= 0. \end{aligned}$$

References

[1] W. Decker, G. -M. Greuel, G. Pfister, and H. Schönemann, SINGULAR 4-0-2 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de (2015).

[2] D. Grayson and M. Stillman, *Macaulay2, a software system for research in algebraic geometry*, Available at http://www.math.uiuc.edu/Macaulay2/.

[3] Maple 2016. Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario.

[4] Wolfram, Mathematica, 10.3 ed., Wolfram Research, Inc., Champaign, Illinois, 2015, https://www.wolfram.com.

Session 5

Computational Algebraic Geometry, and Post-Quantum Cryptography - Multivariate Public Key Cryptography

Session chairs:

Jintai Ding
University of Cincinnati, USA

Shuhong Gao
Clemson University, USA

Yossi Perez
Jerusalem College of Technology, Israel

Ludvic Perret
Universite Pierre et Marie Curie, Paris, France

Daniel Smith-Tone
University of Louiseville, USA

Tsuyoshi Takagi
Kyushu University, Japan

Length-based attacks on a cryptosystem based on polycyclic groups

David Garber

The Anshel-Anshel-Goldfeld (AAG) key-exchange protocol was implemented and studied with the braid groups as its underlying platform. The length-based attack, introduced by Hughes and Tannenbaum, has been used to cryptanalyze the AAG protocol in this setting. Eick and Kahrobaei suggest to use the polycyclic groups as a possible platform for the AAG protocol.

In a joint work with **Delaram Kahrobaei** and **Ha T. Lam**, we apply several known variants of the length-based attack against the AAG protocol with the polycyclic group as the underlying platform. The experimental results show that, in these groups, the implemented variants of the length-based attack are unsuccessful in the case of polycyclic groups having high Hirsch length. This suggests that the length-based attack is insufficient to cryptanalyze the AAG protocol, when implemented over this type of polycyclic groups. It has to be mentioned that Kotov and Ushakov recently cryptanalyzed this cryptosystem.

Moreover, we compare *for the first time* between the success rate of the different variants of the length-based attack. These experiments show that, in these groups, the memory length-based attack introduced by Garber, Kaplan, Teicher, Tsaban and Vishne does better than the other variants proposed thus far in this context.

I will start my talk by describing the polycyclic groups and the AAG cryptosystem. Then, I will present the different variants of the length-based attack and the experimental results we have achieved.

On an efficient digital signature for the age of quantum computers

Y. Peretz[1] and N. Granot[2]

[1] *Senior Lecturer at the Computer Sciences Department, Lev Academic Center, Jerusalem, Israel. yosip@g.jct.ac.il*
[2] *Student at the Computer Sciences Department, Lev Academic Center, Jerusalem, Israel. neriagr@gmail.com*

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]). For digital signatures based on multivariate system of equations see e.g. [10] and [11].

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 Smart Cards, 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, two pubic-key encryption schemes (called TP-I and TP-II) were defined in [8], having the following features:

- ♣ The security of the schemes is based on provable NP-complete problem. Thus, the suggested schemes fit to the age of post-quantum cryptography.

- ♣ The schemes involves truly (pseudo) random choice of the coefficients of the core equations and thus can have no vulnerable hidden structure.

- ♣ The schemes are very flexible in the ability of matching the security level to the needs and to the given computing power.

- ♣ The schemes 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).

♣ The schemes has a very fast encryption and decryption time. They have several magnitudes of improvement over the RSA and they outperform the AES for equivalent level of security.

♣ The 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 the research of [8].

Based on the TP-I pubic-key encryption scheme introduced in [8], in the current lecture we suggest a new digital signature. The security and performance of the suggested digital signature and the comparison with other multivariable based existing digital signature schemes, will also be discussed.

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).

[10] J. Patarin, N. Courtois and L. Goubin, *QUARTZ, 128-Bit Long Digital Signatures*, CTRSA 2001, LNCS vol. 2020, pp. 282-297, Springer 2001.

[11] J. Ding and D. S. Schmidt, *Rainbow, a new multivariable polynomial signature scheme*, ACNS 2005, LNCS vol. 3531, pp. 164-175, Springer 2005.

A New Quartic Multivariate Cryptosystem

Lih-Chung Wang

National Dong Hwa University, Taiwan, R.O.C., lcwang@gms.ndhu.edu.tw

We propose a new quartic multivariate cryptosystem, which is a generalization of TRMC with the aide of medium field trick. The new encryption scheme has the remedy for the weakness of the original TRMC. However, the large key size of a quartic system is unavoidable. In fact, the main method to improve security can be applied to other cryptosystems. Hence, we wish that the idea we propose can help to reduce the difficulty for creating secure encryption system.

Let F be the finite field of Z_{17} or Z_{19}. Let ϕ_1 be a random quadratic map from F^4 to F^4. Let $\phi_2, \phi_3, \phi_4, \phi_5$, be random quadratic maps from F^4 to F^8. Let L_1 and L_2 be random linear maps from F^4 to F^8. Let Q_1, Q_2, Q_3 and Q_4 be 4 random quadratic polynomials with 30 variables over F. The central map of our scheme is a quartic system of 36 polynomials with 30 variables. The public key is the composition of the central map and two invertible affine maps, one is before and one is after the central map. The private key is these three maps. The following is the 36 polynomials with 30 variables.

The first 4 quartic polynomials with 30 variables is

$$\phi_1(Q_1, Q_2, Q_3, Q_4)$$

.

The other 32 polynomials is the following.

$$X_1 *_L C_3 + X_2 *_L C_4 + \phi_2(Q_1, Q_2, Q_3, Q_4)$$

$$X_1 *_L C_4 + \phi_3(Q_1, Q_2, Q_3, Q_4)$$

$$X_2 *_L C_3 + \phi_4(Q_1, Q_2, Q_3, Q_4)$$

$$(TRM(X_1) + L_1(Q_1, Q_2, Q_3, Q_4)) *_L L_2(Q_1, Q_2, Q_3, Q_4) + X_2 *_L C_4 + \phi_5(Q_1, Q_2, Q_3, Q_4)$$

where $*_L$ is the multiplication of the degree 8 extension field L of the field F, X_1 is an element in L which 8 components are linear combinations of first 7 variables out of the 30 variables, X_1 is an element in L which 8 components are linear combinations of second 7 variables out of the 30 variables, C_3 and C_4 are elements composed of 8 triangle-like cubic polynomials and $TRM(X_1)$ is an element composed of 8 triangle-like quadratic polynomials of the first 7 variables.

During the talk, we will give the encryption and decryption details and discuss how to resist all known attacks to multivariate encryption systems.

References

[1] L. Bettale, J.-C. Faugère, L. Perret *Cryptanalysis of the TRMS signature scheme of PKC'05.* Proceedings of the Cryptology in Africa 1st international conference on Progress in cryptology. Springer-Verlag, (2008).

[2] J.-C. Faugère. *A New Efficient Algorithm for Computing Gröbner Bases (F4).* Journal of Pure and Applied Algebra, 139(1-3):61-88, (1999).

[3] J.-C. Faugère, and L. Perret. *Cryptanalysis of $2R^-$ schemes.* Advances in Cryptology - CRYPTO 2006, Lecture Notes in Computer Science, vol. 4117, pp. 357-372, (2006).

[4] PA. Fouque, L. Granboulan and J. Stern. *Differential cryptanalysis for multivariate schemes.* ADVANCES IN CRYPTOLOGY - EUROCRYPT 2005, PROCEEDINGS, Lecture Notes in Computer Science Vol. 3494 pp. 341-353,(2005).

[5] F. Levy-dit-Vehel, J.-C. Faugère, and L. Perret *Cryptanalysis of MinRank* CRYPTO 2008: Advances in Cryptology,PROCEEDINGS, Lecture Notes in Computer Science Vol.5157 pp 280-296, (2008).

[6] J. Patarin, *Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt 88*, CRYPTO 95, LNCS vol. 963, pp. 248-261 (1995).

[7] L.-C. Wang and F. Chang. *Tractable Rational Map Cryptosystem.* Cryptology ePrint archive, Report 2004/046, available at http://eprint.iacr.org.

[8] L.-C. Wang, Y.-H. Hu, F.-P. Lai, C.-Y. Chou, and B.-Y. Yang. *Tractable Rational Map Signature.* International Workshop on Theory and Practice in Public Key Cryptography (PKC'05), Lecture Notes in Computer Science, vol. 3386, Springer-Verlag, pp. 244-257, (2005).

[9] L.-C. Wang, B.-Y. Yang, Y.-H. Hu and F.-P. Lai *A "Medium-Field" Multivariate Public-Key Encryption Scheme.* CT-RSA 2006: Topics in Cryptology, PROCEEDINGS, Lecture Notes in Computer Science Vol.3860 pp 132-149 (2006).

Fast construction of a lexicographic Gröbner basis of the vanishing ideal of a set of points

X. Dahan[1]

[1] *Ochanomizu University, Japan, dahan.xavier@ocha.ac.jp, xdahan@gmail.com*

Problem Given a set V of Zariski-closed points lying in $\bar{k}^n$, $\bar{k}$ an algebraic closure of a base field of interest k, its *vanishing ideal* $I(V) \subset k[X_1,\ldots,X_n]$ is the radical, 0-dimensional ideal of polynomials vanishing on V. We are interested in constructing a minimal lexicographic Gröbner basis $\mathscr{G}$ of $I = I(V)$.

Result The main outcome is Result 1. below. In HPC, a complexity analysis often precedes an implementation, and a challenge is indeed that benchmarks meet the expected complexity bounds. This is where lies this work (A preliminary implementation is available in Maple, but cannot be qualified as HPC currently).

Notations Lex, LexGB stands for lexicographic and lexicographic Gröbner basis respectively. Given a set $E \subset k[X_1,\ldots,X_n]$, then $E_{\leq \ell}$ denotes the set $E \cap k[X_1,\ldots,X_\ell]$. The projection of n-uplet that forgets the last $n-i$ coordinates is denoted π_i, that is $\pi_i(a_1,\ldots,a_n) = (a_1,\ldots,a_i)$.

1. There is a minimal lexicographic Gröbner basis $\mathscr{G}$ whose any of its polynomial can be computed in $O(\mathsf{A}(D_1) + \mathsf{A}(D_2) + \cdots + \mathsf{A}(D_n))$ arithmetic operations where $D_i = |\pi_i(V)| = \dim_k(k[X_1,\ldots,X_i]/I_{\leq i})$, and $\mathsf{A}(d)$ is the number of arithmetic operations over k necessary to build Lagrange idempotents of d points by using sub-product tree techniques ($\mathsf{A}(d) = \mathsf{M}(d)\log(d)$ using Schönhage-Strassen fast multiplication, or $d^2\log(d)$ using naive polynomial multiplication).

2. the polynomials in $\mathscr{G}$ present a special structure, sort of redundant factors that allows to recycle already computed polynomials and Lagrange cofactors (and those computed in the sub-product trees) to considerably lower the number of arithmetic operations to compute new polynomials in $\mathscr{G}$.

3. Any polynomial in $\mathscr{G}$, say w.l.o.g. in $k[X_1,\ldots,X_n] \setminus k[X_1,\ldots,X_{n-1}]$, verifies a generalization of Gianni-Kalkbrener theorem: if $\alpha \in \pi_\ell(V)$ is such that $\deg_{X_{\ell+1}}(g(\alpha, X_{\ell+1},\ldots,X_n)) < \deg_{X_{\ell+1}}(g)$, then $g(\alpha, X_{\ell+1},\ldots,X_n) = 0$.

4. $\mathscr{G}$ is not the reduced Gröbner basis in general, hence has more coefficients, but its coefficients are smaller.

5. to V, we first build its *decomposition points tree* $\mathscr{T}(V)$. The *arithmetic* complexity for solving "Problem" depends only of the shape of this tree (of course not the case for the bit complexity where the bit-size of the input points matters also).

Brief overview of previous works The above results are related to a number of previous works. We only refer to the most relevant ones that put into perspective the above statements. The numbering below refers to that of above.

1. Lederer [10] who has produced the most accomplished interpolation formulas focuses on the *reduced* Gröbner basis, which complicates his task quite considerably. This leaves a sharp complexity analysis quite difficult — indeed there is none; this stems for the fact that many additional polynomials must be computed on demand to cancel too large monomials. The reduced lexGB has a less satisfactory specialization property (see [1, 8]).

Before it was understood that the configuration of points in V could give the set of standard monomials for the lexicographic oder (Cf. [3, 13, 6, 5]), algorithms based on linear algebra were predominant. They give roughly an $O(nD^3)$ [2, 14] arithmetic cost (but are *not* constrained to the lex order).

A related problem concerns the computation of a separating basis of the vector space $k[X_1,\ldots,X_n]/I$. By "separating" we mean polynomials $\{p_v\}_{v\in V}$ such that $p_v(w)=\delta_{vw}$ (Kronecker symbol). Such a basis is closely related to multivariate Lagrange bases: Lundqvist [12] claims a cost of $O(D^2)$ points, but using fast interpolation it can be reduced to a complexity similar to that stated in Result 1. above. As for Hermite interpolation, in [11] linear algebra exploits the possibly very low displacement rank of the interpolating matrix to propose $O((\tau+3)D^2)$ (for Vandermonde we have $\tau=2$ hence of the same order of Lagrange interpolation with naive multiplication).

2. Starting with Lazard's structural theorem ([9], lexGB in two variables), several authors have shown that a somewhat comparable result holds for more than two variables (to cite a few [13], and implicitly in [5, 10, 6]), at least in the radical 0-dimensional case. However, few, if none, considered the relationship between factors of two different polynomials in $\mathscr{G}$. This is a key point to recycle computations and to dramatically decrease the complexity, even if it is not easy to quantify.

3. The stability of Gröbner bases under specialization refers to the fact that a specialized Gröbner basis remains a Gröbner basis of the specialized ideal. Beyond the seminal Gianni-Kalkbrener result [7], Becker [1] then Kalkbrener [8] showed that whenever a degree decrease occurs after specialization, then the polynomial reduces to zero modulo the other polynomials. As stated, the specific Gröbner

basis that we construct verifies a stronger property: no degree decrease, or else it specializes to zero, as in Gianni-Kalkbrener's theorem.

4. The maximal bit-size among all coefficients of polynomials appearing in $\mathscr{G}$ can be estimated to be *roughly* in $O(nD^2h^2)$ where h is the maximal bit-size of the components of input points. This strategy follows that of [4]. Again, obtaining such a sharp result for the reduced lexGB is not easy.

5. this is interesting if we see the formula constructing the basis $\mathscr{G}$ as an algebraic circuit that computes the polynomials in $\mathscr{G}$. This circuit depends only of the shape of the tree.

Implementation We have implemented *naively* the interpolation formula that computes $\mathscr{G}$ in Maple and will show experimental results that illustrate all the points mentioned above.

References

[1] T. Becker. Gröbner bases versus D-Gröbner bases, and Gröbner bases under specialization. *Applicable Algebra in Engineering , Communications and Computing*, 5:1–8, 1994.

[2] B. Buchberger and H. Möller. The construction of multivariate polynomials with preassigned zeros. In *Lecture Notes in Computer Science (EUROCAM'82)*, volume 144, pages 24–31, London, UK, 1982.

[3] L. Cerlienco and M. Mureddu. From algebraic sets to monomial linear bases by means of combinatorial algorithms. *Discrete Mathematics*, 139(1-3):73–87, 1995.

[4] X. Dahan and É. Schost. Sharp estimates for triangular sets. In *ISSAC '04: Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, pages 103–110. ACM Press, 2004.

[5] B. Felszeghy, B. Ráth, and L. Rónyai. The lex game and some applications. *J. of Symbolic Comput.*, 41(6):663 – 681, 2006.

[6] S. Gao, V. Rodrigues, and J. Stroomer. Gröbner basis structure of finite sets of points. http://www.math.clemson.edu/~sgao/pub.html, 2003. Preprint (16 pages).

[7] P. Gianni. Properties of Gröbner bases under specialization. In J.H. Davenport, editor, *In Proc. of EUROCAL'87*, Lecture Notes in Computer Science (378), pages 293–297. Springer, Berlin, 1987.

[8] M. Kalkbrener. On the stability of Gröbner bases under specialization. *J. Symbolic Comput.*, 24(2):51–58, 1997.

[9] D. Lazard. Ideal bases and primary decomposition: case of two variables. *J. Symbolic Comput.*, 1(3):261–270, 1985.

[10] M. Lederer. The vanishing ideal of a finite set of closed points in affine space. *J. of Pure and Applied Algebra*, 212:1116–1133, 2008.

[11] Na Lei, Yuan Teng, and Yu-xue Ren. A fast algorithm for multivariate hermite interpolation. *Applied Mathematics-A Journal of Chinese Universities*, 4(29):438–454, 2014.

[12] Samuel Lundqvist. Vector space bases associated to vanishing ideals of points. *Journal of Pure and Applied Algebra*, 214(4):309 – 321, 2010.

[13] M. G. Marinari and T. Mora. A remark on a remark by Macaulay or enhancing Lazard structural theorem. *Bull. Iranian Math. Soc.*, 29(1):1–45, 85, 2003.

[14] M.G. Marinari, H. M. Moeller, and T. Mora. Gröbner bases of ideals defined by functionals with an application to ideals of projective points. *Applicable Algebra in Engineering, Communication and Computing*, 4(2):103–145, 1993.

Session 6

Computer Algebra for Applied Physics

Session chairs:

Avi Karsenty
Department of Physics/Electro-Optics, Jerusalem College of Technology, Israel

David Kamoun
Department of Physics/Electro-Optics, Jerusalem College of Technology, Israel

Avraham Chelly
Faculty of Engineering, Bar Ilan University, Ramat Gan, Israel

Yaakov Mandelbaum
Jerusalem College of Technology, Israel

Itzhak Leichter
Department of Physics/Electro-Optics, Jerusalem College of Technology, Israel

Naftali Schweitzer

Department of Physics/Electro-Optics, Jerusalem College of Technology, Israel

Computer Algebra in Theoretical Physics

E.S. Cheb-Terrab[1]

[1] *Maplesoft R&D, Canada, ecterrab@maplesoft.ca*

Generally speaking, physicists still experience that computing with paper and pencil is in most cases simpler than computing on a Computer Algebra worksheet. On the other hand, recent developments in the Maple system have implemented most of the mathematical objects and mathematics in theoretical physics computations, and have dramatically approximated the notation used in the computer to the one used with paper and pencil, diminishing the learning gap and computer-syntax distraction to a strict minimum. In this talk, the Physics project at Maplesoft is presented and the resulting Physics package is illustrated by tackling problems in classical and quantum mechanics, using tensor and Dirac's Bra-Ket notation, general relativity, including the equivalence problem, and classical field theory, deriving field equations using variational principles.

References

[1] L.D. Landau and E.M, Lifshitz, *Course of Theoretical Physics*, Elsevier (1975).

[2] E.S. Cheb-Terrab, *Mini-Course: Computer Algebra for Physicists*. Mapleprimes `http://www.mapleprimes.com/posts/200223-MiniCourse-Computer-Algebra-For-Physicists` (2014).

Sliding of a Block on the Plane with Variable Coefficient of Friction: Simulation with Mathematica

Alexander N. Prokopenya

Warsaw University of Life Sciences – SGGW, Warsaw, Poland,
alexander_prokopenya@sggw.pl

Dry friction of solids is often encountered both in engineering practice and in our everyday life. Its study has a long history and many different models were proposed to explain its physical properties (see [1, 2]). In spite of a complexity of the dry friction as a physical phenomenon, its basic laws are known since the works of Amontons and Coulomb (see [3, 4]), and they give simple quantitative estimates of the friction forces which are widely used in engineering applications. Remind that a body sliding on a rough surface is acted on by a friction force that is parallel to the surface and is directed opposite to the velocity of the body. The friction force does not depend on the area of contact of the body and the surface and is proportional to the normal reaction force, where the proportionality constant is known as the coefficient of friction.

In the case when the body contacts the surface in one or two points one can easily obtain the equations of motion of the system because the points of application of the friction forces and the normal forces are known. But in case of a finite dimension of the contact area the normal force is inevitably a distributed force. It does not essential matter if the body slides on the surface with constant coefficient of friction but may become very important when the body crosses a boundary of two domains with different coefficients of friction.

As an example let us assume that a homogeneous rectangular block sliding on a smooth horizontal plane enters the domain with nonzero coefficient of friction. To write the equations of motion and to analyze dynamics of the block we need to know a distribution of the normal force along the block length. In the present talk we propose the following model of dry friction of the block and the plane. First, we assume that deformation of the block is negligible and it may be considered as a rigid body. Besides, the elastic properties of the plane are the same in all its points and does not depend on the coefficient of friction. In the framework of such a model one can consider that a density of the normal force is a linear function $N(x) = kx + b$, where x is a local coordinate measured along the block from its center of mass, and $k,\ b$ are the two constants which may be found from the conditions of the block motion without rotation.

Note that the normal force and the friction force become dependent of position of the body at the plane and this complicates the equations of motion considerably.

And one has to combine symbolic and numerical calculations for solving these equations. However, such a problem can be efficiently solved with some modern computer algebra system.

Doing necessary calculations, we analyze motion of the system and demonstrate some peculiarities of the block sliding on the plane with variable coefficient of friction in the case when the area of the bodies contact is finite. We use the computer algebra system Mathematica (see [5]) to do all relevant calculations and visualization of the results.

References

[1] D. Dowson. *History of tribology*, Longman, London (1979)

[2] Bo N.J. Persson. *Sliding friction. Physical principles and applications*, Springer-Verlag, Berlin, Heidelberg (2000)

[3] P. Painlevé, *Leçons sur l'integration des équations differentielles de la mécanique et applicatiòns*, Paris, Hermann (1895).

[4] Le x. Anh, *Dynamics of mechanical systems with Coulomb friction*, Springer-Verlag, Berlin, Heidelberg (2003).

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

Normal forms of perturbed Hamiltonians: symbolic computation and applications

M. Avendaño-Camacho[1], J. A. Vallejo[2], Yu. Vorobiev[1]

[1] *Universidad de Sonora, México, misaelave@mat.uson.mx,yurimv@guaymas.uson.mx*
[2] *Universidad Autónoma de San Luis Potosí, México, jvallejo@fc.uaslp.mx*

For simplicity, we will consider Hamiltonians defined on the symplectic manifold $\mathbb{R}^{2n}$, with coordinates (q^j, p_j) $(1 \leq j \leq n)$, endowed with the canonical form $w = \mathrm{d}p_j \wedge \mathrm{d}q^j$, although all the results remain valid for an arbitrary symplectic manifold (and even arbitrary Poisson ones).

Given a Hamiltonian system defined by the Hamiltonian function $H \in \mathscr{C}^\infty(\mathbb{R}^{2n})$,

$$\begin{aligned} \dot{q}^j &= \frac{\partial H}{\partial p_j} \\ \dot{p}_j &= -\frac{\partial H}{\partial q^j}\,, \end{aligned} \tag{1}$$

two of the main goals in the theory of dynamical systems are the determination of possible closed, stable orbits, and the computation of adiabatic invariants (of course, taking for granted the impossibility of solving (1) explicitly). Of particular interest is the case in which the Hamiltonian H is a perturbation of an integrable one, say, $H = H_0 + \sum_{j=1}^{n} \varepsilon^j H_j$. A widely used procedure to study it, consists in writing the Hamiltonian in the so-called *normal form*, that is, as a formal series [7, 8, 9]

$$H = \sum_{j=0}^{\infty} \varepsilon^j N_j \tag{2}$$

where $N_0 = H_0$, and each N_j commutes with the unperturbed Hamiltonian,

$$\{H_0, N_j\} = 0\,.$$

Notice that transforming to the normal form introduces a (possibly infinite) family of first integrals which are not present in the original system. These additional, spurious symmetries must be removed [6], and this is usually done by restricting the system to a reduced phase space through symplectic (singular) reduction. A number of well-known theorems are available to do this [4, 5, 10, 9, 11].

Even more, truncation of the formal series (2) is the starting point for proving the existence of closed orbits [4, 6], and the computation of adiabatic invariants [2]. In the talk, I will show how to use a Maxima package to compute normal forms as in (2), illustrating the procedure with some examples based on joint work with Yu. Vorobiev and M. Avendaño-Camacho [1, 2, 3].

References

[1] M. Avendaño-Camacho, J. A. Vallejo, Yu. Vorobjev, A simple global representation for second-order normal forms of Hamiltonian systems relative to periodic flows, J. Phys. A: Math. Theor. 46 (2013) 395201

[2] M. Avendaño-Camacho, J. A. Vallejo, Yu. Vorobiev, Higher order corrections to adiabatic invariants of generalized slow-fast Hamiltonian systems, J. Math. Phys. 54, 082704 (2013).

[3] M. Avendaño-Camacho, J. A. Vallejo, Yu. Vorobiev,A perturbation theory approach to the stability of the Pais-Uhlenbeck oscillator. arXiv:1703.08929 [math-ph].

[4] R. C. Churchill, M. Kummer and D. L. Rod, On averaging, reduction, and symmetry in Hamiltonian systems. J. of Di . Eqs. 49 (1983) 359–414

[5] R. H. Cushman and L. Bates, Global aspects of classical integrable systems. Birkhauser, Basel, 1997.

[6] R. Cushman, Geometry of perturbation theory, in 'Deterministic Chaos in General Relativity'. D. Hobill, A. Burd, A.A. Coley (eds.) Nato Science Series B, Vol. 332, Springer Verlag (1993) 89–101.

[7] A. Deprit, Canonical transformation depending on a small parameter, Celest. Mech., 1 (1969) 13–30.

[8] A. A. Kamel, Perturbation method in the theory of nonlinear oscillations, Celest. Mech., 3 (1970) 90–106.

[9] K. R. Meyer, Normal forms for Hamiltonian systems, Celest. Mech., 9 (1974) 517–522

[10] J. Moser, Regularization of Kepler's problem and the averaging method on a manifold, Comm. on Pure and Appl. Math., 23, Issue 4 (1970) 609–636.

[11] J. P. Ortega and T. Ratiu, Momentum Maps and Hamiltonian Reduction. Springer Verlag, Basel (2004).

Singular Perturbad Vector Fields (SPVF) Applied To Combusion of Spray of Diesel Droplets

O. Nave[1]

[1] *Jerusalem College of Technology, Israel, {naveof}@gmail.com*

In our research we present the concept of singularly perturbed vector field method (SPVFM) [1], and its application to thermal explosion of diesel spray combustion. Given a system of governing equations, which consist of hidden Multiscale variables, the SPVF method transfer and decompose such system to fast and slow singularly perturbed subsystems (SPS). The resulting subsystem enable us to understand better the complex system, and simplify the calculations. later powerful analytical, numerical and asymptotic methods (e.g method of integral (invariant) manifold (MIM) [2], the homotopy analysis method (HAM) etc.) can be applied to each subsystem. In this paper we compare the results obtained by the methods of integral invariant manifold and SPVFM apply to spray (polydisperse) droplets combustion model.

The algorithm for SPVFM: 1: Select the linear points $\Gamma = \{x_1, ..., x_N\}$ where $N >> n$, uniformly distribute in the domain V by using quasi-stochastic distribution.
2: Compute the mean value of the vector filed over the point from step 1: $\bar{F} = \frac{1}{N}\sum_{i=1}^{N} F(x_i)$,
3: Define the so-called the control set (the separated set) as follow:
$\{x_i \in \Gamma : \|F(x_i)\| > \|\bar{F}\|, i = 1, ..., k \cdot n\}$, where $k >> n$,
4: Build the approximation of T_i for $i = 1, ..., k$ based of the control set from step 3 as: $\vec{x}_i^* = \left\{x_{(i-1)\cdot n+1}, ..., x_{i\cdot n}\right\}$,
5: Select only the reference set from step 4 which have $|Det(\vec{x}_i^*)|$ above the average level over all subsets: $\Omega = \frac{1}{k}\sum_{i=1}^{k} |Det(\vec{x}_i^*)|$, and denoted by:
$\{\vec{x}_i : x_{i_k} \in \Gamma : |Det(\vec{x}_i)| \geq \Omega, i = 1, ..., k\}$ the control set of ordered subsets of length n from set Γ,
6: Compute the eigenvalues of T_{i^*}, i.e., $\lambda_j(T_{i^*})$, $j = 1, ..., n$,
7: The final reference sequence $\vec{x}_{i^*} = \left\{x_{(i^*-1)\cdot n+1}, ..., x_{i\cdot n}\right\}$ and the approximation of $T = T_{i^*}$ is found simultaneously as:
$T = T_{i^*} = \left(F(x_{(i^*-1)\cdot n+1}), ..., F(x_{i^*\cdot n})\right)(\vec{x}_{i^*})^{-1}$. by the maximum gap for the given dimension of the reduced model n_s as:
$i^* : \varepsilon = min_i \left(|\lambda_{n_s+1}(T_{i^*})| / |\lambda_{n_s}(T_{i^*})|\right)^{-1}$.

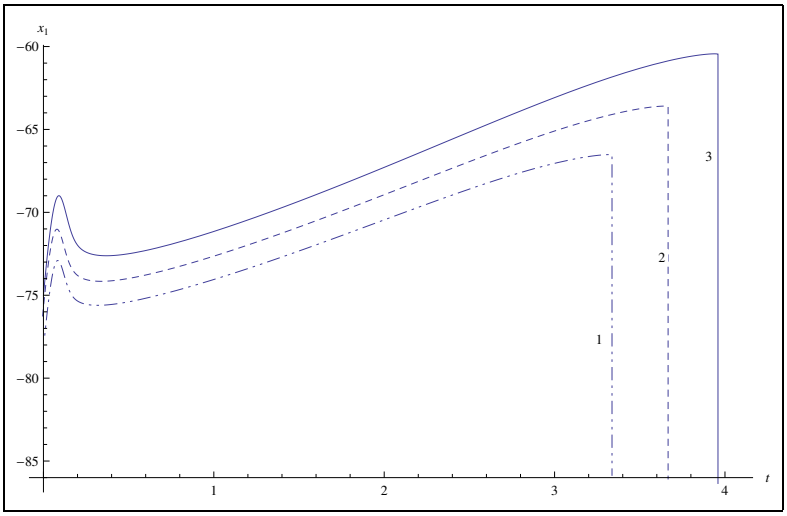


Figure 1: The solution profiles of x_1 the transform model after changing the coordinate..

1 Results

We present in this section the results of the algorithm for SPVFM

References

[1] V. Bykov, , I Goldfarb and V Gol?dshtein, *Singularly perturbed vector fields*, Journal of Physics: Conference Series 55, pp. 28?44 (2006).

[2] M.R. Roussel, S.J. Fraser, Invariant manifold methods for metabolic model reduction, Chaos 11, 196-206, (2001)

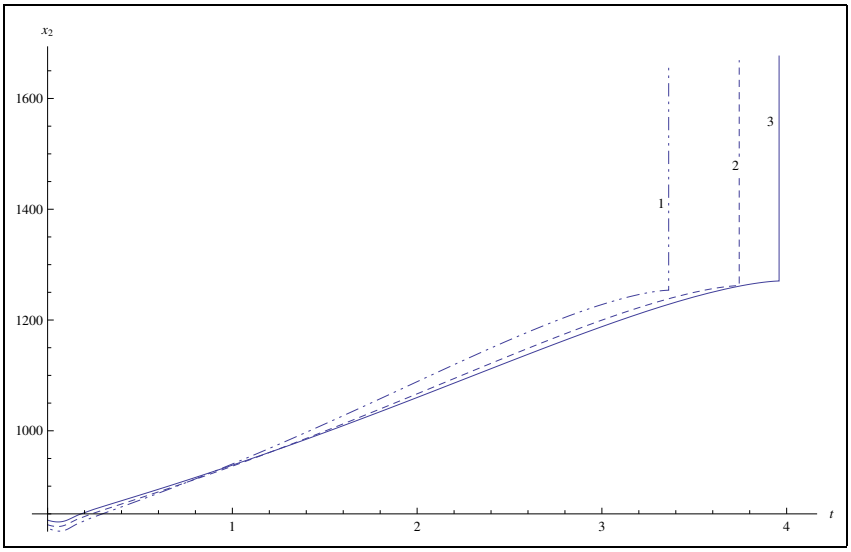


Figure 2: The solution profiles of x_2 the transform model after changing the coordinate.

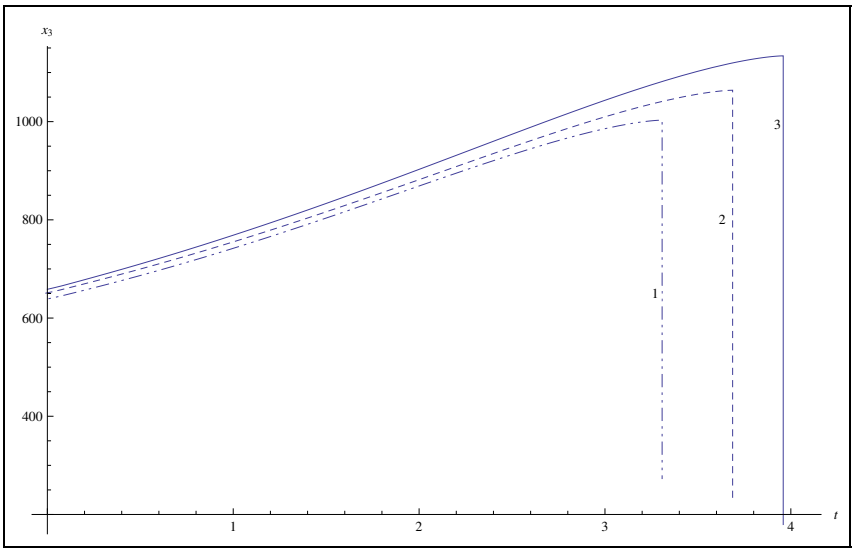


Figure 3: The solution profiles of x_3 the transform model after changing the coordinate.

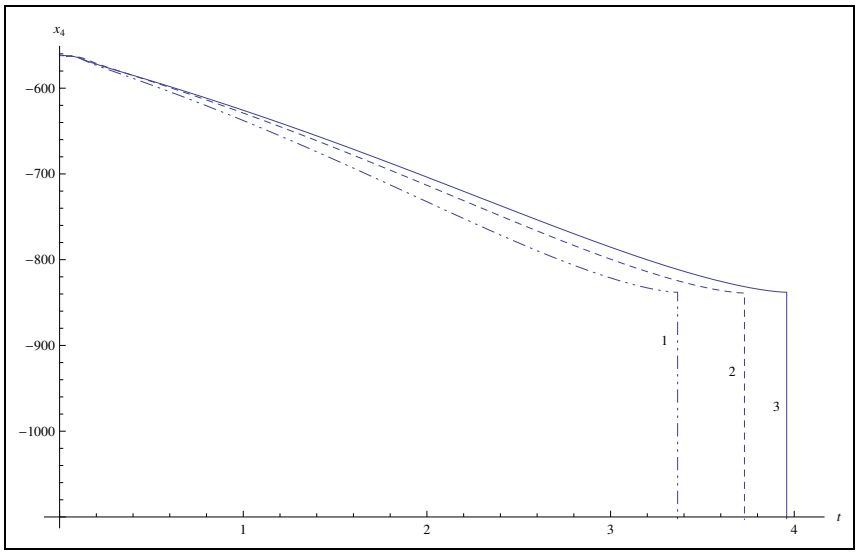


Figure 4: The solution profiles of x_4 the transform model after changing the coordinate.

Computer algebra in nanotechnology: Modelling of Nano Electro-Optic Devices using Finite Element Method (FEM)

Avi Karsenty and Yaakov Mandelbaum

Jerusalem College of Technology

We will discuss the simulation of Silicon-based light-emitting and photodetectors nano-devices using computer algebra. These devices couple the hyperbolic equations of Electromagnetic Radiation, the parabolic equations of Heat Conduction, the elliptic equations describing electric potential, and the eigenvalue equations of Quantum Mechanics - with the nonlinear drift-diffusion equations of the semiconductor physics. These must be solved subject to generally mixed Dirichlet-Neumann boundary conditions in three-dimensional geometries.

Comsol Multiphysics modelling software is employed integrated with Matlab-Simulink and Zemax. The physical equations are discretized on a mesh using the Galerkin Finite Element Method (FEM), and to a lesser extent the method of Finite Volumes (FVM). The equations can be implemented in a variety of forms such as directly as a PDE, or as variational integral, the so called weak form. Boundary conditions may also be imposed directly or using variational constraint and reaction forces. Both choices have implication for convergence and physicality of the solution. The mesh is assembled from triangular or quadrilateral elements in two-dimensions, and hexahedral or prismatic elements in three dimensions, using a variety of algorithms. Solution is achieved using direct or iterative linear solvers and non-linear solvers. The former are based on conjugate gradients, the latter generally on Newton-Raphson iterations.

The general framework of FEM discretization, meshing and solver algorithms will be presented together with techniques for dealing with challenges such as multiple time scales, shocks and non-convergence; these include load-ramping, segregated iterations, and adaptive meshing.

Algebraic Processing of Sequential Fluoroscopy Images for Quantitative Evaluation of Partial Obstruction of the Upper Urinary Tract

T. Yeshua[1], O. Gleisner [2], V. Neeman[1], R. Lederman[3],
M. Duvdevani[4], I. Leichter [1,3]

[1] *Dept. of Electro-optics, Lev Academic center, Jerusalem, Israel*
[2] *Dept. of Electro-Optics Engineering, Ben Gurion University, Beer-Sheva, Israel*
[3] *Dept. of Radiology. Hadassah University Hospital, Jerusalem, Israel*
[4] *Dept. of Urology. Hadassah University Hospital, Jerusalem, Israel*

Objective: To develop a novel method for the quantitative evaluation of partial obstruction of the upper urinary tract in patients who have undergone percutaneous nephrolithotomy (PCNL). For this purpose, sequential fluoroscopic images obtained during a postoperative nephrostogram were processed in order to calculate the residual amount of contrast material in the renal collecting system and evaluate the urine flow rate.

Background: Obstruction of the upper urinary tract is a blockage that inhibits the free flow of urine from the kidneys, through the ureters to bladder. It is a common urological pathology that may lead to renal dysfunction, and when untreated, it can lead to infection and progressive atrophy of the kidney [1]. It is mostly caused by the formation of stones in the renal pelvis. Failure of normal drainage of urine from the kidney collecting system typically causes hydronephrosis - distension and dilation of the renal pelvis and calyces [2]. To resolve the obstruction, the kidney stones are usually removed by a minimally-invasive procedure called PCNL [3]. In a nephrostogram [4], which is routinely performed on the second postoperative day, contrast material is inserted into the renal collecting system in order to demonstrate passage of contrast material to the bladder by fluoroscopy [5]. However, this procedure does not allow calculating quantitative parameter reflecting the urine flow rate. The algebraic processing of fluoroscopy images may replace renal scintigraphy, which involves the use of radioactive materials, and is used today to diagnose obstruction of the upper urinary [6]. Material and methods: Study cohort consisted of 27 patients (13 females, 14 males) with a mean age of 48.7 ± 13.2 years, who underwent a PCNL. Post-operative nephrostograms of 12 patients showed no evidence of hydronephrosis, while in 15 patients, hydronephrosis was demonstrated. Sequential fluoroscopic images obtained during the nephrostogram were analyzed in order to estimate the urine flow rate from the renal collecting system. An algorithm was developed in the MATLAB (MathWorks, USA) computing environment to calculate the gray level values of the contrast material in each sequential image.

Based on this calculation, the residual amount of contrast material within the renal collecting system was evaluated at a given time. Algebraic evaluation shows that the amount of contrast material should decrease exponentially with time. The calculated values of the amount of contrast material were plotted as function of time to yield the clearance curve and the time at which half of the contrast material had been drained from the renal collecting system. Results: The clearance curve based on calculating the residual amount of contrast material in the renal pelvis fitted, as expected, an exponential regression function with a mean correlation coefficient of 0.954 ± 0.008 $(p < 0.02)$. From the exponential function the decay constant, τ was calculated to yield $t_{1/2}$ and the flow rate in the renal pelvis was evaluated. Since obstruction of the upper urinary tract is associated with hydronephrosis, the flow rate of cases with evidence of hydronephrosis was compared to that of normal cases. For cases with hydronephrosis, the mean $t_{1/2}$ value calculated from the fitted exponential regression curve (6.37 ± 1.79 minutes) was markedly longer than the mean $t_{1/2}$ value of normal cases (1.25 ± 0.87 minutes).

Conclusions: Processing of images acquired during a nephrostogram provides a quantitative assessment for the urine flow rate in the kidney collecting system. The flow rate in cases with evidence of hydronephrosis was markedly lower, with a 5 times longer $t_{1/2}$ than in normal cases. Therefore, this method may provide a quantitative parameter for diagnosing partial obstruction of the upper urinary tract.

References

[1] J. Hall and K.D. Linton. *Obstruction of the upper and lower urinary tract*, Surgery (Elsevier), 26(5), pp. 197-202 (2008).

[2] W.E. Goodwin, W.C. Casey and W. Woolf. *Percutaneous trocar (needle) nephrostomy in hydronephrosis*, JAMA, 157(11), pp. 891-894 (1955).

[3] S.R. Patel and S.Y. Nakada. *The modern history and evolution of percutaneous nephrolithotomy*, J. Endourol., 29, pp. 153-157 (2015).

[4] K.M. Al-Kohlany, A.A. Shokeir, A. Mosbah, T. Mohsen, A.M. Shoma, I. Eraky, M. El-Kenawy, and H.A. El-Kappany. *Treatment of complete staghorn stones: a prospective randomized comparison of open surgery versus percutaneous nephrolithotomy*, J. Urol., 173(2), pp. 469-473 (2005).

[5] M. Kirac, A. Tepeler, C. Guneri, S. Kalkan, S. Kardas, A. Armagan, and H. Biri. *Reduced radiation fluoroscopy protocol during retrograde intrarenal surgery for the treatment of kidney stones*, Urology Journal, 11(3), p.1589 (2014).

[6] A.T. Taylor. *Radionuclides in nephrourology, part 1: Radiopharmaceuticals, qualitycontrol, and quantitative indices*. Journal of Nuclear Medicine, 55(4), pp. 608-615 (2014).

Computer algebra in satellite image processing

David Kamoun, Yishai Arieli, Shaul Golan, Moshe Hababou and Shalom Dimant

Jerusalem College of Technology, paulk@g.mail.jt.ac.il

Computer algebra is ubiquitously used in satellite imaging (see [1]) and in particular in the autonomous exploitation of satellite images. A couple of examples developed in our Remote Sensing Laboratory are given (as in [2]), one related to the automatic atmospheric correction of images, the other related to the deconvolution of images to improve the image exploitation process. These applications have been carried out with the standard use of MATLAB, an important and efficient tool for student projects.

References

[1] R.C. Gonzalez, R.E. Woods and S.L. Eddins Digital Image Processing using MatLab, Pearson Prentice Hall, Upper Saddle River, NJ, USA (2003).

[2] K. Tempfli, N. Kerke, G. Huurneman and L. Janssen. Priciples of Remote Sensing, ITC Educational Textbook Series 2, Enschede, The netherlands (2009).

On the Applicability of Pairwise Separations Method in Astronomy: Influence of the Noise in Data

J. Benjamin[1], D. Walker[1], A. Mylläri[1], T.Mylläri[1]

[1] *St. George's University, Grenada, West Indies {amyllari}@sgu.edu*

Small number of objects poses often a problem in the analysis of large-scale structure of the Universe, especially if one is interested in studying fractal structures – estimating the fractal dimension or similar characteristics. So, pairwise separations method that uses not coordinates of objects (n sets of coordinates for n objects) but pairwise distances ($n(n-1)/2$ distances) looks very attractive. We studied the applicability of the pairwise separations method in astronomy. Description of the method and some applications of it in astronomy can be found in [1] and [2]. This method may be used, in particular to analyze fractal sets: for a fractal set with Hausdorff-Bezicovich dimension D, the distribution of pairwise distances $f(l)$ behaves asymptotically as $f(l) \propto l^{D-1}$ for small l.

Since large enough data set is needed to estimate the fractal dimension, using this method looks promising, especially in the case when using a small sample of data - as pairwise separations method indicates, pairwise distances are used rather than points; thus, dealing with $n(n-1)/2$ distances as compared to n original data points.

In [2], the authors made simulations to estimate applicability of the method, however, large noiseless data sets for experiments were used. Here, we use more realistic data for simulations. Iterated function systems (IFS, see, e.g., [3]) were used to generate model fractal sets, then noise was added to the data. Estimates of fractal dimension using pairwise-separations method were conducted where results were compared with the dimension of the attractor of the IFS and with estimates of the box-counting dimension. In the simulations, classic 2D fractals - Sierpinsky carpet and Sierpinsky gasket as well as 3D fractals of the Menger Sponge family were used. These simulations were executed using computer algebra system Wolfram Mathematica 11 to generate fractal sets and estimate dimension of these sets using pairwise separations method. To test applicability of the method in practice, noise to the data was added in order to evaluate how it affects the results. A series of simulations were also done without noise to test the influence of the sample size. Results of the tests are illustrated in Tables 1 and 2, and examples of simulations are shown on Figures 1 and 2 below.

As highlited in the noiseless cases the method works quite well, even for small n. However with the addition of noise the picture changes. This could be expected since the noise influences small distances. Since observational data have limited

accuracy, one must be coucious when using pairwise separations method in practice, especially with small and noisy datasets.

noise level \ n	100	200	500	1000
0	1.58 ± 0.10	1.58 ± 0.06	1.58 ± 0.02	1.58 ± 0.01
1%	1.59 ± 0.11	1.58 ± 0.06	1.58 ± 0.03	1.58 ± 0.01
2.5%	1.60 ± 0.12	1.61 ± 0.06	1.62 ± 0.02	1.61 ± 0.01
5%	1.66 ± 0.15	1.67 ± 0.07	1.70 ± 0.03	1.68 ± 0.02
10%	1.74 ± 0.14	1.77 ± 0.08	1.78 ± 0.04	1.77 ± 0.02

Table 1: Estimated dimension for the Sierpinsky gasket (dimension 1.58).

noise level \ n	100	200	500	1000
0	1.78 ± 0.16	1.87 ± 0.09	1.88 ± 0.03	1.88 ± 0.02
1%	1.78 ± 0.20	1.88 ± 0.09	1.88 ± 0.09	1.88 ± 0.02
2.5%	1.79 ± 0.19	1.89 ± 0.10	1.90 ± 0.04	1.89 ± 0.02
5%	1.83 ± 0.19	1.93 ± 0.11	1.94 ± 0.04	1.90 ± 0.02
10%	1.92 ± 0.21	1.99 ± 0.13	2.00 ± 0.04	1.94 ± 0.02

Table 2: Estimated dimension for the Sierpinsky carpet (dimension 1.89).

References

[1] A.A.Raikov, V.V.Orlov, and O.B.Beketov. Inhomogeneities in the Spatial Distribution of Gamma-Ray Bursts. *Astrofysics*, 53(3):396–408, 2010.

[2] A.A. Raikov and V.V. Orlov. Method of pairwise separations and its astronomical applications. *Mon. Not. R. Astron.Soc.*, 418:2558–2546, 2011.

[3] Heinz-Otto Peitgen, Hartmut Jürgens, Dietmar Saupe *Chaos and Fractals: New Frontiers of Science.* Springer, 2004, 864 pp.

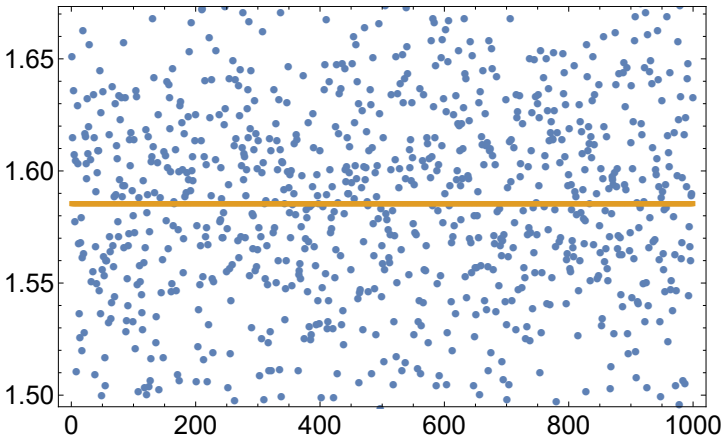


Figure 1: Estimated dimensions for 1000 simulations of the Sierpinsky gasket. 200 points, no noise added.

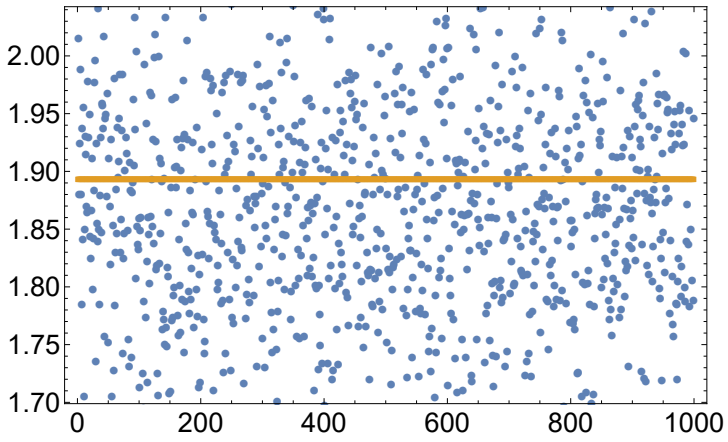


Figure 2: Estimated dimensions for 1000 simulations of the Sierpinsky carpet. 200 points, 2.5 % noise added.

Session 7

Computer Algebra for Dynamical Systems and Celestial Mechanics

Session chairs:

Victor Edneral
Lomonosov Moscow State University, Russia

Aleksandr Mylläri
St. Georges University, Grenada

Valery Romanovski
University of Maribor, Slovenia

Nikolay Vassiliev
V.A. Steklov Institute of Mathematics of the Russian Academy of Sciences, Russia

The construction of averaged planetary motion theory by means computer algebra system Piranha

A.S. Perminov, E.D. Kuznetsov

Ural Federal University, Ekaterinburg, Russia, perminov12@yandex.ru, eduard.kuznetsov@urfu.ru

The investigation of planetary systems dynamical evolution is one of important problems of celestial mechanics. In this work we consider the construction of averaged semi-analytical motion theory for a planetary system with four planets. We need to obtain motion equations in time-averaged orbital elements. The use of these elements allows to eliminate short-periodic perturbations in the planetary motion and to construct the motion theory for a long-time period.

For our purposes the non-averaged Hamiltonian of the four-planetary problem is written in Jacobi coordinates.

$$h = -\sum_{i=1}^{4} \frac{M_i \kappa_i^2}{2a_i} + \mu \times Gm_0 \Big\{ \sum_{i=2}^{4} \frac{m_i (2\mathbf{r}_i \mathbf{R}_i + \mu R_i^2)}{r_i \tilde{R}_i (r_i + \tilde{R}_i)} - \sum_{i=1}^{4} \sum_{j=1}^{i-1} \frac{m_i m_j}{|\rho_i - \rho_j|} \Big\}. \quad (1)$$

Here

$$\mathbf{R}_i = \sum_{k=1}^{i} \frac{m_k}{\bar{m}_k} \mathbf{r}_k, \quad \tilde{R}_i = \sqrt{r_i^2 + 2\mu \mathbf{r}_i \mathbf{R}_i + \mu^2 R_i^2}, \quad (2)$$

and

$$|\rho_i - \rho_j| = \mathbf{r}_i - \mathbf{r}_j + \mu \sum_{k=j}^{i-1} \frac{m_k}{\bar{m}_k} \mathbf{r}_k, \quad (3)$$

where numbers i and j satisfy a condition $1 \leq j < i \leq 4$; ρ_k is the barycentric radius vector of k-th planet, $\mathbf{r}_k$ is Jacobi radius vector of the same planet; μm_k is the mass of the planet in items of the Sun mass m_0, $\bar{m}_k = 1 + \mu m_1 + \ldots + \mu m_k$, $M_i = m_i \bar{m}_{i-1} / \bar{m}_i$, $\kappa_i^2 = Gm_0 \bar{m}_i / \bar{m}_{i-1}$ is the gravitational parameter and μ is the small parameter of the problem, which is equal to the ratio of the sum of planetary masses and the mass of the star. For instance, if we take into account the Solar system then the value of μ can take equal to 0.001.

The first sum in (1) is the undisturbed part of the Hamiltonian, which describes the Keplerian motion of planets around the Sun. The expression in figure brackets is the disturbing function. Double sum in (1) is the main part of the disturbing function, which describes the interaction between planets.

Further it is expanded into the Poisson series in orbital elements of the Poincare second system. This system has only one angular element – mean longitude. It

allows to simplify an angular part of the series expansion. The elements of the second Poincare system are defined through classical Keplerian elements by the following way

$$L_i = M_i\sqrt{\kappa_i^2 a_i}, \quad \lambda_i = \Omega_i + \omega_i + l_i,$$

$$\xi_{1i} = \sqrt{2L_i(1-\sqrt{1-e_i^2})}\cos(\Omega_i+\omega_i),\ \xi_{2i} = \sqrt{2L_i\sqrt{1-e_i^2}(1-\cos I_i)}\cos\Omega_i,$$

$$\eta_{1i} = -\sqrt{2L_i(1-\sqrt{1-e_i^2})}\sin(\Omega_i+\omega_i),\ \eta_{2i} = -\sqrt{2L_i\sqrt{1-e_i^2}(1-\cos I_i)}\sin\Omega_i,$$

where M_i is normalized mass, κ_i^2 is normalized gravitational parameter, a_i – semi-major axis of the orbital ellipse, e_i – eccentricity of this ellipse, I_i – inclination of the orbital plane relative to the reference plane, quantities Ω_i, ω_i, l_i are longitude of the ascending node, argument of the pericenter and mean anomaly of the planet respectively.

The elements of second Poincare system are canonical and three pairs of these are canonical conjugated as the momentum and its the corresponding coordinate, namely L and λ, ξ_1 and η_1, ξ_2 and η_2.

The Hamiltonian of the planetary problem can be expanded into the Poisson series in the following form

$$h = h_0 + \mu h_1 = h_0 + \sum_{k,n} A_{kn} x^k \cos(n\lambda), \tag{4}$$

where h_0 is the undisturbed Hamiltonian, μh_1 is the disturbing function, A_{kn} is numerical coefficients, x^k is the product of Poincare elements with corresponding degrees, cosine is represent the angular part of the series, $n\lambda$ is the linear combination of mean longitudes of planets.

In our work the expansion of the Hamiltonian is constructed up to the second degree of the small parameter. The algorithm of the Hamiltonian expansion is described more detail in [1].

The averaged Hamiltonian of the four-planetary problem is constructed by the Hori-Deprit method. This averaging method based on using of Poisson brackets formalism and theory of Lie transformation. It is characterized by efficiency and very ease for the computer implementation. More detail see in [2].

Let us divide the variables of the problem into two parts – slow variables $x = (L, \xi_1, \eta_1, \xi_2, \eta_2)$ and fast λ. The rates of change for slow variables are proportionally the small parameter while the rates of change for fast variables are proportion to the mean motions. After averaging transformation with respect to the mean longitudes λ, the Hamiltonian is written in averaged slow variables X as the series of the small parameter

$$H(X) = H_0 + \sum_{m=1}^{\infty} \mu^m H_m(X), \tag{5}$$

where quantities H_m are obtained from the main equation of the Hori–Deprit method

$$H_m(X) = h_m + \sum \frac{1}{r!} \{T_{j_r}, \{\cdots, \{T_{j_1}, h_{j_0}\}\}\}. \tag{6}$$

The summation is over the domain $0 \le j_0 \le m-1$; $j_1, j_2, \cdots, j_r \ge 1$; $\sum_{s=0}^{k} j_s = m$; $1 \le r \le m$. The figure brackets is Poisson brackets with respect to the Poincare elements. h_m are items of not averaged Hamiltonian h, and the generating function of the transformation between osculating and averaging elements is defined as

$$T(X,\Lambda) = \sum_{m=1}^{\infty} \mu^m T_m(X,\Lambda). \tag{7}$$

Averaged motion equations can be obtained using Poisson brackets

$$\frac{\mathrm{d}X}{\mathrm{d}t} = \{H, X\}, \quad \frac{\mathrm{d}\Lambda}{\mathrm{d}t} = \{H, \Lambda\}. \tag{8}$$

The transformation from osculating to averaged elements gives by functions for the change of variables u_m, v_m

$$X = x + \sum_{m=1}^{\infty} (-1)^m \mu^m u_m(x,\lambda), \quad u_m = \sum \frac{1}{r!} \{T_{j_r}, \{\cdots, \{T_{j_1}, X\}\}\} \tag{9}$$

$$\Lambda = \lambda + \sum_{m=1}^{\infty} (-1)^m \mu^m v_m(x,\lambda), \quad v_m = \sum \frac{1}{r!} \{T_{j_r}, \{\cdots, \{T_{j_1}, \Lambda\}\}\} \tag{10}$$

where the summation over the domain $j_1, j_2, \cdots, j_r \ge 1$; $\sum_{s=0}^{k} j_s = m$; $1 \le r \le m$.

All analytical transformations in our work are implemented by means of computer algebra system Piranha [3]. Piranha is an echeloned Poisson series processor. It is new, specified, high-efficient C++ code for analytical manipulations with different series. Piranha is freeware, object-oriented and cross-platform software. For the convenience Piranha has Python user-interface which is the set of some Python libraries. This program was written by Francesco Biscani from Heidelberg University, Germany.

Piranha can works with multivariable polynomials, Poisson series and echeloned Poisson series (Poisson series with denominators). It is possible to use real or rational types of series coefficients and powers of variables. In this work we used echeloned Poisson series with rational coefficients and powers that allows to eliminate rounding errors and provides arbitrary precision of resulting series.

In the process Piranha showed a high speed of analytical transformations and ability to work with the series of a very large number of terms (up to $10^8 - 10^9$ terms).

Finally we have applied our averaged motion theory to the investigation of orbital evolution of Solar system's giant planets. The results of numerical integration of the averaged motion equations for Sun - Jupiter - Saturn - Uranus - Neptune's system on a time interval of 10 billion years is considered. The obtained results show qualitative agreement with other motion theories.

References

[1] A.S. Perminov and E.D. Kuznetsov, *Expansion of the Hamiltonian of the planetary problem into the Poisson series in elements of the second Poincare system*, Solar System Research. **49**, 6, pp. 430-441 (2015).

[2] A.S. Perminov and E.D. Kuznetsov, *The Hori-Deprit method for averaged motion equations of the planetary problem in elements of the second Poincare system*, Solar System Research. **50**, 6, pp. 426-436 (2016).

[3] F. Biscani, *The Piranha computer algebra system*. https://github.com/bluescarni/piranha (2017).

Study of nonlinear degenerated ODEs

Victor F. Edneral

Lomonosov Moscow State University, Russian Federation, edneral@theory.sinp.msu.ru
Peoples' Friendship University of Russia, edneral_vf@rudn.university

The report describes power transformations of autonomous degenerated ODEs polynomial systems which reduce such systems to a non-degenerate form. There is an example of building exact first integrals of motion of some planar degenerate system in a closed form by the normal form method.

We consider an autonomous degenerated ODEs system of the form

$$\begin{array}{l} dx/dt = -y^3 - bx^3y + a_0x^5 + a_1x^2y^2 \ , \\ dy/dt = cx^2y^2 + x^5 + b_0x^4y + b_1xy^3 \ . \end{array} \tag{1}$$

The following result was proven in [4, 5].

Theorem 1.*In the case* $D \stackrel{\text{def}}{=} (3b+2c)^2 - 24 \neq 0$*, system (1) is locally integrable only if the number* $(3b-2c)/\sqrt{D}$ *is rational.* When $c = 1/b$ this condition is satisfied. So we put below $c = 1/b$.

Systems with a nilpotent matrix of the linear part were thoroughly studied by Lyapunov and others. In system (1) there is no linear part and the first approximation is not homogeneous. This is the simplest case of a planar system without linear part and with Newton's open polygon [1, 2] consisting of a single edge. In general case such problems have not been studied.

In the report we demonstrate the technique based on the Power Geometry method [3] which allows to transform the problem above to a set of problems with a nilpotent matrix of the linear parts. Really, by using the power transformation [3, 4]

$$x = uv^2, \quad y = uv^3 \tag{2}$$

and the time rescaling $u^2v^7dt = d\tau$, we obtain system (1) in the form

$$\begin{array}{ll} du/d\tau = & -3u - [3b + (2/b)]u^2 - 2u^3 + (3a_1 - 2b_1)u^2v + \\ & (3a_0 - 2b_0)u^3v \ , \\ dv/d\tau = & v + [b + (1/b)]uv + u^2v + (b_1 - a_1)uv^2 + (b_0 - a_0)u^2v^2 \ . \end{array} \tag{3}$$

Under the power transformation (2) the point $x = y = 0$ blows up into two straight invariant lines $u = 0$ and $v = 0$. Along the line $u = 0$ the system (3) has a single stationary point $u = v = 0$. Along the second line $v = 0$ this system has four elementary stationary points

$$u = 0, \quad u = -\frac{1}{b}, \quad u = -\frac{3b}{2}, \quad u = \infty \ . \tag{4}$$

For studying system (1) near the point $x = y = 0$ one needs investigate it near all stationary points (4) of the system (3).

Realization of this approach allowed to get six exact families of the first integrals of motion of (1) in finite terms. Each family is function of two from five parameters of system (1).

The author was supported by the grant NSh-7989.2016.2 of the President of Russian Federation and by the Ministry of Education and Science of the Russian federation (Agreement number 02 A03.21.0008).

References

[1] A.D. Bruno, Analytical form of differential equations (I,II), Trudy Moskov. Mat. Obsc. 25, (1971) 119-262, 26 (1972) 199-239, (Russian) = Trans. Moscow Math. Soc. 25 (1971) 131-288, 26, (1972) 199-239 (English)

[2] A.D. Bruno, Local Methods in Nonlinear Differential Equations, Nauka, Moscow, 1979 (Russian) = Springer-Verlag, Berlin, 1989 (English)

[3] A.D. Bruno, Power Geometry in Algebraic and Differential Equations, Fizmatlit, Moscow, 1998 (Russian) = Elsevier Science, Amsterdam, 2000 (English)

[4] A.D.Bruno, V.F.Edneral, On Integrability of a Planar ODE System near a Degenerate Stationary Point, in V.P.Gerdt et.al. (Eds.) Proceedings of the CASC 2009, Springer-Verlag series: LNCS 5743 (2009) 45-53 A.D.Bruno and V.F.Edneral, On Integrability of a Planar System of ODEs Near a Degenerate Stationary Point, Journal of Mathematical Sciences **166** no. 3 (2010) 326-333

[5] A.D. Bruno, V.F. Edneral, Possibility of Additional Solutions of the Degenerate System Near Double Degeneration at the Special Value of the Parameter, in V.P.Gerdt et.al. (Eds.) Proceedings of the CASC 2013, Springer-Verlag series: LNCS 8136 (2013) 75-87

Symbolic Dynamics in the Equal Mass Free-Fall Three-Body Problem: Analysis of Ergodic Components

A.Mylläri[1], N. Vassiliev[2], T. Mylläri[1], A. Myullyari[3]

[1] *St. George's University, Grenada, West Indies {amyllari}@sgu.edu*
[2] *V.A. Steklov Institute of Mathematics of the Russian Academy of Sciences, St. Petersburg, Russia*
[3] *Accendo Data LLC Coral Springs, Florida, USA*

We consider equal mass free-fall three-body problem. Symbolic sequences are constructed numerically using close binary approaches. Shannon entropy is estimated for each sequence as well as length of the sub-sequence that provides maximum value of the entropy for each sequence. Here, we analyse some features revealed on the diagram maximum value of the entropy - corresponding length of the sub-sequence (see Fig. 3 below).

Equal mass free-fall three-body problem is convenient for study since it allows easy visualization of initial configuration: if we place two bodies in the points $(-0.5;0)$ and $(0.5;0)$, then all possible configurations will be covered if we place the third body inside the region D bounded by two straight line segments and arc of the unit circle centered at $(-0.5,0)$ (Fig. 1) [1].

Raspberry Pi cluster was used for numerical integration of trajectories and construction of symbolic sequences, Wolfram Mathematica is used to analyze sequences received. We used symplectic code by Seppo Mikkola (Tuorla Observatory, University of Turku) [2] for numerical simulations.

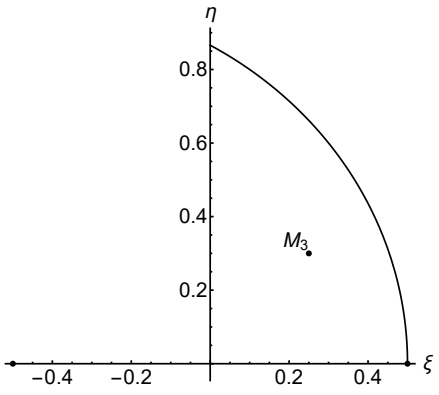


Figure 1: Agekian-Anosova region D.

We scan Agekian-Anosova region D and construct symbolic sequences of length 50 using close binary approaches – we detect minimum distance between two bodies, and corresponding symbol is the number of the distant body. Thus, our symbols are from the alphabet {1, 2, 3}. Some systems disrupt fast, so some sequences are short. Some systems live long (e.g. metastable systems [3]), so corresponding sequences are long. To have a reasonable computing time, we constructed symbolic sequences length 50. Since we are interested in the analysis of active three-body interactions, we consider sub-sequences of each of these sequences, increasing the length step-by-step, calculate entropy for each of these sub-sequences, and find maximum value of these entropies. Maximum value (and moment of time/length of the sub-sequence) correspond to the stage of active interaction between bodies.

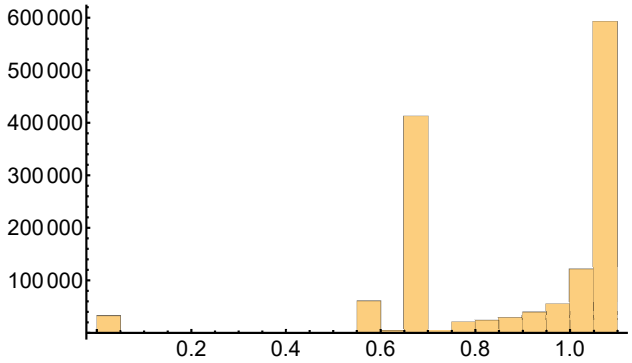


Figure 2: Histogram of maximum values of the entropy.

Histogram of maximum values of the entropy shows two distinct modes (Fig. 2). Left mode corresponds to the sequences with only two symbols equally represented: Entropy[{1, 2, 1, 2}]=0.693147. Second mode corresponds to the sequences where all three symbols are equally presented: Entropy[{1, 2, 3, 1, 2, 3}]=1.09861. Interesting structures can also be seen on the scatterplot of maximum values of the entropy - corresponding length of symbolic sequence in the neighborhood of these modes (Fig. 3). We analyze these structures and trace coresponding initial conditions in the Agekian-Anosova region D.

Authors acknowledge Dr. Ian V. J. Murray, Dept Physiology and Neuroscience, St. George's University for the collaborative purchase of Wolfram *Mathematica*.

References

[1] Agekian, T.A. and Anosova, J.P. 1967, Astron. Zh., 44, 1261

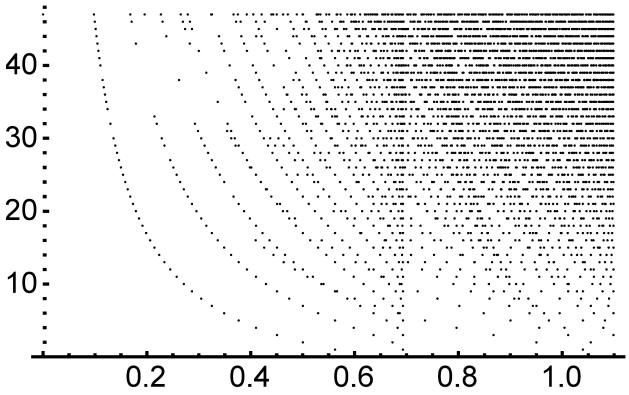


Figure 3: Scatterplot of maximum values of the entropy - corresponding length of symbolic sequence.

[2] Mikkola, S. and Tanikawa, K. 1999, Celest. Mech. Dyn. Astron., 74, 287-295.

[3] Martynova A.I., Orlov V.V., Rubinov A.V.,2003, MNRAS, 344, 1091

On the Stability Criteria for Hierarchical Three-Body Systems

A.Pasechnik[1], M. Valtonen,[2] , A. Mylläri[3]

[1] *Tuorla Observatory, Department of Physics and Astronomy, University of Turku, Finland*
[2] *Finnish Center for Astronomy with ESO (FINCA), Piikkiö, Finland*
[3] *St. George's University, Grenada, West Indies {amyllari}@sgu.edu*

It is often important to decide if a given hierarchical triple star system is stable over an extended period of time. Here, we test a stability criterion, modified from earlier work, where we use the closest approach ratio Q of the third star to the inner binary centre of mass in their initial osculating orbits. We study by numerical integration the orbits of over 100,000 triple systems varying masses, outer and inner eccentricities, and inclinations i. The definition of the instability is either the escape of one of the bodies, or the exchange of the members between the inner and outer systems. The dependence of Q_{st} (the smallest Q value which allows the system to be stable over $N = 10,000$ revolutions of the initial outer orbit) on the mass values and on the outer orbit eccentricity e_{out} is briefly explored, and it is also found to agree with the analytical theory. The final stability limit formula is

$$Q_{st} = 10^{1/3} A[(f \cdot g)^2/(1-e_{out})]^{1/6}$$

where the coefficient $A = 1$ should be used in N-body experiments, and $A = 2$ when the absolute long term stability is required. The functions $f(e_{in}, cosi)$ and $g(m_1, m_2, m_3)$ are

$$\begin{aligned} f(e_{in}, \cos i) &= \left\{ 1 - \frac{2}{3} e_{in} \left[1 - \frac{1}{2} e_{in}^2 \right] - 0.3 \cos i \left[1 \right. \right. \\ &- \left. \left. \frac{1}{2} e_{in} + 2 \cos i \left(1 - \frac{5}{2} e_{in}^{3/2} - \cos i \right) \right] \right\}. \end{aligned}$$

$$g(m_1, m_2, m_3) = \left(1 + \frac{m_3}{m_1 + m_2} \right).$$

At the limit of $e_{in} = i = m_3 = 0$, $f \cdot g = 1$.

The study of Markov processes on 3D Schur graph

V. Duzhin[1], N. Vasilyev[2]

[1] *Saint Petersburg Electrotechnical University, Russia, vduzhin.science@gmail.com*
[2] *St.Petersburg department of Steklov Institute of mathematics RAS, Russia, vasiliev@pdmi.ras.ru*

The three-dimensional Schur graph is an infinite graded graph whose vertices are three-dimensional strict Young diagrams (strict planar partitions). Young graph and Schur graph are related to various problems of asymptotic combinatorics. Some of these problems show the connection between the combinatorics of these graphs and special Markov processes on them. From this point of view, the most important Markov processes are those which generate a central measure [1].

A central measure is a measure where the probabilities of different paths between given pair of diagrams are the same. For two-dimensional case there exists a central process called Plancherel process. Papers [2, 3, 4] were devoted to investigation of sequences produced by Plancherel process on two-dimensional Young and Schur graphs. Unfortunately, there are no known central processes on three-dimensional Young and Schur graphs. Markov processes on three-dimensional Young graph which generate asymptotically central measure were investigated in [5, 6]. These are so-called pseudo-Plancherel processes.

Here we construct an analogous process on three-dimensional Schur graph. In order to show the asymptotic centrality, we study the ratios of probabilities of different paths between a pair of diagrams. We define the normalized dimension for three-dimensional strict Young diagrams. We investigate both random and greedy paths for pseudo-Plancherel processes on Schur graph. A greedy path is a deterministic sequence of diagrams built in the following way: on each step the box with the maximum possible probability is added to the diagram. Also we investigate the growth and oscillations of normalized dimensions along greedy trajectories of processes. We study the limit shape of a strict three-dimensional diagram produced by pseudo-Plancherel process.

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] N. N. Vasilyev and V. S. Duzhin, *A study of the growth of maximal and typical normalized dimensions of strict Young diagrams*, J. Math. Sci. 216 (2016) 53-64, doi: [doi:10.1007/s10958-016-2887-x]

[4] V. S. Duzhin and N. N. Vasilyev, *Asymptotic behavior of normalized dimensions of standard and strict Young diagrams - growth and oscillations*, J. Knot Theory Ramifications 25, 1642002 (2016) [16 pages] DOI: http://dx.doi.org/10.1142/S0218216516420025

[5] N. N. Vasiliev, V. S. Duzhin, *Numerical investigation of the asymptotics of the probabilities of paths in a Markov process on the 3D Young graph close to a central one*, Representation theory, dynamical systems, combinatorial and algoritmic methods. Part XXVII, Zap. Nauchn. Sem. POMI, 448, POMI, St. Petersburg, 2016, 69-79

[6] V. Duzhin, N. Vasilyev, *Modeling of an Asymptotically Central Markov Process on 3D Young Graph*, N. Math.Comput.Sci. (2017). doi:10.1007/s11786-017-0314-4

Session 8

Algorithmic Combinatorics

Session chairs:

Christoph Koutschan
RICAM, Austrian Academy of Sciences, Linz, Austria

Computing Automorphism Groups of Designs - a Way to Produce New Symmetric Weighing Matrices

Giora Dula[1], Assaf Goldberger[2], Yossi Strassler[3]

[1]*Netanya Academic College, Israel, giora@netanya.ac.il*
[2]*Tel Aviv University, Israel assafg@post.tau.ac.il*
[3] *Dan Yishai, Israel danyishay@gmail.com*

A weighing matrix of size n and weight k, also denoted as $W(n,k)$ is a $\{0,1,-1\}$-$n \times n$ matrix W such that $WW^T = kI_n$. Two weighing matrices V and W are said to be isomorphic (or Hadamard equivalent), if there exist two signed permutation matrices P and Q auch that $W = PVQ$. In this work we have developed an efficient algorithm, implemented in sage, to find an isomorphism between weighing matrices if one exists. Our algorithm works well with designs in general, and in fact the case of weighing matrices is more difficult because of the presence of signs. In particular, we are able to compute automorphism groups of weighing matrices. One application of this is to search for a (anti-)symmetric weighing matrix in a class of a given matrix W. If a matrix W is isomorphic to W^T, then we compute the isomorphism $PWQ = W^T$, and the automorphism group of W. If a (anti-)symmetric representative of this class exists, then for a specific isomorphism $P'WQ' = W^T$, it will happen that $P'W$ is (anti-)symmetric. We have been able to implement this to a newly discovered weighing matrix $W(23,16)$ and obtain a symmetric matrix with the same parameters.

Our algorithm uses certain strong invariants that may separate nonisomorphic classes. If two matrices V and W have the same invariant, then we have some initial clue on the desired permutations. Then, after considerably small enumeration we are able to reduce the problem to unsigned permutations. Then we use an algorithm based on the singular value decomposition to discover the full permutations.

One interesting (future) application of automorphisms, may apply to the problem of 'coloring' a matrix. Namely, if we are given only the elementwise absolute value $|W|$ of a weighing matrix W, then we need to recover W from $|W|$, at least if we believe that W has rich automorphism group. If we compute the group $Aut(|W|)$, then we need to find a signed permutation group G and an embedding $G \to Aut(|W|)$. If we find such G, then its orbits give us much information as to how to color $|W|$. Finding such G is a problem in Group Theory and it is interesting to understand how the orthogonality of W projects on this Group-Theoretic problem.

Patterns in Random Permutations

Chaim Even-Zohar[1]

[1] *University of California, Davis, USA, chaim@math.ucdavis.edu*

The density at which fixed patterns occur in large permutations has received much attention in Combinatorics. Pattern densities give rise to extremal questions, and play a role in the construction of limiting objects for permutations, and in permutation property testing. The case where some patterns are avoided is studied extensively.

We report on the study of pattern densities in *random* permutations. Our work extends the discussion by Janson, Nakamura and Zeilberger in Section 4 of [1]. In particular, we address the question in its closing paragraph, on the emerging general structure. To this end, we analyze the distribution of pattern densities using representations of the symmetric group.

This viewpoint of pattern densities provides a unified framework for several measures from non-parametric statistics, such as Kendall's τ, Spearman's ρ and some two-sample independence tests. It is also related to the spectral analysis of statistical data on nonabelian groups, as introduced by Diaconis [2].

We present some definitions before stating the main questions and results. Let $\pi \in S_n$ and let $k \leq n$. Consider all $\binom{n}{k}$ restrictions of π to k entries $\pi_{a_1} \dots \pi_{a_k}$ where $a_1 < a_2 < \ldots < a_k$. The relative ordering of such k values induces a *pattern* $\sigma \in S_k$. For example, the restriction of $\pi = \underline{4}\,\underline{1}\,2\,\underline{5}\,3$ to the marked entries induces the 3-pattern $\sigma = 2\,1\,3$.

Let the *density* of $\sigma \in S_k$ be $P_\sigma(\pi) := N_\sigma(\pi)/\binom{n}{k}$, where $N_\sigma(\pi)$ is the number of times σ occurs as a k-pattern in π. The *k-profile* of π is the $k!$-dimensional vector of all k-pattern densities $\mathbf{P}_k(\pi) := (P_\sigma(\pi))_{\sigma \in S_k}$. When $\pi \in S_n$ is sampled uniformly at random, we denote its k-profile by $\mathbf{P}_{kn}$.

A first observation is that $\mathbf{P}_{kn} \to \mathbf{U}_k := \left(\frac{1}{k!}, \ldots, \frac{1}{k!}\right)$ in probability as $n \to \infty$. It is hence interesting to understand how the k-profile deviates from this limit. What is the order of magnitude of $(\mathbf{P}_{kn} - \mathbf{U}_k)$ as n grows? What directions in the $k!$-dimensional space are typical of this vector? Does it have a natural decomposition into lower-dimensional components? What is the shape of the distribution when properly normalized?

It turns out that linear representations of S_k provide some answers to these questions. Recall that each simple representation R^λ corresponds to an integer partition $k = \lambda_1 + \ldots + \lambda_\ell$ where λ_1 is the largest. Consider the subspace spanned by the matrix elements $(R^\lambda_{ij}(\sigma))_{\sigma \in S_k}$ viewed as $k!$-dimensional vectors.

Orthogonal projections on these subspaces provide an initial decomposition of the k-profile. We show that the component that corresponds to R^λ has order of magnitude $n^{(\lambda_1-k)/2}$ asymptotically as n grows. One can use this decomposition to *normalize* the distribution of the profile, multiplying the different components by the appropriate powers of n.

We also show that components of different orders are asymptotically uncorrelated, in the sense that the cross-covariance matrix of the two normalized vectors converges to zero. This indicates that representations of the symmetric group may also help to *diagonalize* the profile's distribution.

Indeed, for $k \leq 6$ we found specific unitary matrix representations of S_k, whose matrix elements diagonalize the normalized distribution of the k-profile. This means that its covariance matrix, with respect to that basis, converges to a diagonal with positive entries. We hope to extend this result to every k in future work.

The above results were discovered by computer exploration. Our starting point was the interpolation of the profile's covariance matrix, symbolically as rational functions of n. This allowed us to extract several leading coefficients that determined the asymptotic behavior, and to look at their diagonal forms.

The full analysis and verification of the cases $k = 3,4,5,6$ were undertaken by explicit computation of appropriate unitary representations, that seem to have interesting properties by their own.

References

[1] S. Janson, B. Nakamura and D. Zeilberger, *On the asymptotic statistics of the number of occurrences of multiple permutation patterns*, J. Comb. **6**, pp. 117-143 (2015).

[2] P. Diaconis, *Group representations in probability and statistics*, Inst. Math. Stat. Hayward CA (1988).

Reconstructing Weighing Matrices From Their Automorphism Group

Giora Dula[1], Assaf Goldberger[2], Yossi Strassler[3]

[1]*Netanya Academic College, Israel, giora@netanya.ac.il*
[2]*Tel Aviv University, Israel assafg@post.tau.ac.il*
[3] *Dan Yishai, Israel danyishay@gmail.com*

A weighing matrix of order n and weight k, generally denoted by $W(n,k)$ is a $n \times n$ $\{0,1,-1\}$-matrix W such that $WW^T = kI_n$. We say that two matrices W_1 and W_2 in $W(n,k)$ are (Hadamard) equivalent, if $W_2 = LW_1R$ for monomial matrices L,R. The Automorphism group of a weighing matrix $W \in W(n,k)$ is the group

$$Aut(W) \;=\; \{(L,R)\;|LWR = W,\; L,R \text{ monomial}\}$$

with multiplication given by $(L,R)\cdot(L',R') := (LL',R'R)$.

Suppose now we are only given the group $Aut(W)$ and we would like to reconstruct W from it. Then $Aut(W)$ gives us a lot of information on W: The action of $Aut(W)$ on pairs (i,j), $1 \le i,j \le n$ splits the space of n^2 pairs into orbits, and a single entry in each orbit, determines all remaining entries in the orbit. This suggests a massive reduction in the search space for W.

Moreover, suppose for the moment that $Aut(W)$ acts bi-transitively on the rows of the matrix. Then for any candidate matrix W the resulting Gram matrix WW^T is constant (up to sign) off the diagonal. In particular, this value has fairly good chances to be zero, hence W will be a weighing matrix. Even when it is nonzero, in some cases there are augmenting constructions that can fix the problem.

To obtain such constructions, we first need to construct candidates for the automorphism groups. To this end we begin with two embeddings $L_0,R_0 : G \to S_n$ (considered as action of G on the rows and columns), and then lift them to embeddings $L,R : G \subset B_n$ using Group Cohomology. We now analyze the orbits of the action on pairs of row and column. Some orbits will result in conflicting signs, and must be given the value zero, the other orbits may be given any value in $\{0,1,-1\}$.

This method was applied to various cases: Some well known families such as Payley's Conference and Hadamard Matrices, as well as projective spaces are all a special case of this construction. We have also obtained some seemingly new families. We also can construct matrices from groups that are not doubly transitive.

We obtain gram matrices with some interesting structure, and they can serve as building blocks for weighing matrices.

D-finite Numbers*

Hui Huang, Manuel Kauers

Institute for Algebra, Johannes Kepler University, Linz A-4040, Austria
hui.huang@jku.at, manuel@kauers.de

D-finite functions have been recognized long ago [6, 5] as an especially attractive class of functions. The defining property of a *D-finite* function is that it satisfies a linear differential equation with polynomial coefficients. In a sense, the theory of D-finite functions generalizes the theory of algebraic functions. Many properties enjoyed by the latter carry over to the former.

It is well-known that the class of algebraic numbers and the class of algebraic functions are naturally connected to each other. Motivated by this relation, we have established in [3] a similar correspondence between numbers and the class of D-finite functions, More precisely, we introduced the following class of numbers.

Definition 1 ([3]). *Let R be a subring of $\mathbb{C}$ and let $\mathbb{F}$ be a subfield of $\mathbb{C}$. A number $\xi \in \mathbb{C}$ is called* D-finite *(with respect to R and $\mathbb{F}$) if there exists a convergent sequence $(a_n)_{n=0}^{\infty}$ over R with $\lim_{n\to\infty} a_n = \xi$ and some polynomials $p_0, \ldots, p_r \in \mathbb{F}[n]$, $p_r \neq 0$, not all zero, such that $p_0(n)a_n + p_1(n)a_{n+1} + \cdots + p_r(n)a_{n+r} = 0$ for all $n \in \mathbb{N}$. The set of all D-finite numbers w.r.t. R and $\mathbb{F}$ is denoted by $\mathscr{D}_{R,\mathbb{F}}$.*

It is clear that $\mathscr{D}_{R,\mathbb{F}}$ contains all the elements of R, but it typically contains many further elements. For example, let i be the imaginary unit, then $\mathscr{D}_{\mathbb{Q}(i),\mathbb{Q}(i)}$ contains many (if not all) the periods [4] and, as we will see from Theorem 3, all the values of G-functions [1] as well as many (if not all) regular holonomic constants [2]. In addition, thanks to many mathematicians' work, we can easily recognize that many constants like e, $1/\pi$, Euler's constant γ are D-finite.

The definition of D-finite numbers given above involves two subrings of $\mathbb{C}$ as parameters: the ring to which the sequence terms of the convergent sequences are supposed to belong, and the field to which the coefficients of the polynomials in the recurrence equations should belong. One of the goals of [3] is to investigate how R and $\mathbb{F}$ can be modified without changing the resulting class of D-finite numbers. We have found some interesting properties pursuing this goal. For example, algebraic extensions of $\mathbb{F}$ are useless to extend the class; and it is also not useful to make $\mathbb{F}$ bigger than the quotient field of R. Moreover, we showed that

Theorem 2 ([3]). *For every D-finite number $\xi \in \mathscr{D}_{R,\mathbb{F}}$, there exists $g(z) \in R[[z]]$ D-finite over $\mathbb{F}$ such that $\xi = \lim_{z\to 1^-} g(z)$.*

*The research was funded by the Austrian Science Fund (FWF) under grants Y464-N18, F5004, and W1214-N15 (project part 13).

The above theorem implies that D-finite numbers are computable when the ring R and the field $\mathbb{F}$ consist of computable numbers. Consequently, all non-computable numbers have no chance to be D-finite. Besides these artificial examples, we do not know of any explicit real numbers which are not in $\mathscr{D}_{\mathbb{Q},\mathbb{Q}}$, and we believe that it may be very difficult to find some.

On the other hand, the values D-finite functions can assume at non-singular algebraic points are all D-finite, as indicated by the following theorem.

Theorem 3 ([3])**.** *Let $\mathbb{F}$ be a subfield of $\mathbb{C}$ with $\mathbb{F} \setminus \mathbb{R} \neq \emptyset$ and let R be a subring of $\mathbb{C}$ containing $\mathbb{F}$. Assume that $f(z) \in \mathscr{D}_{R,\mathbb{F}}[[z]]$ is analytic at zero and D-finite over $\mathbb{F}$. Further assume that zero and $\zeta \in \bar{\mathbb{F}}$ are not singularities of an annihilating operator for $f(z)$. Then the derivative $f^{(k)}(\zeta) \in \mathscr{D}_{R,\mathbb{F}}$ for all $k \in \mathbb{N}$.*

We have made some first steps in [3] towards understanding the nature of D-finite numbers. We believe that, similarly as for D-finite functions, the class is interesting because it has good mathematical and computational properties and because it contains many special numbers that are of independent interest. At last, we list some possible directions of future research.

1. After proving Theorem 3, it would be natural to wonder about the values of a D-finite function at singularities of its annihilating operators.

2. It would be interesting to know precisely under which circumstances the multiplicative inverse of a D-finite number is D-finite. Are there choices of R and $\mathbb{F}$ for which $\mathscr{D}_{R,\mathbb{F}}$ is a field?

3. A similar pending analogy concerns compositional inverses. Is it true that the values of compositional inverses of D-finite functions are D-finite numbers?

References

[1] Stéphane Fischler and Tanguy Rivoal. On the values of G-functions. *Comment. Math. Helv.*, 89(2):313–341, 2014.

[2] Philippe Flajolet and Brigitte Vallée. Continued fractions, comparison algorithms, and fine structure constants. In *Constructive, experimental, and nonlinear analysis (Limoges, 1999)*, volume 27 of *CMS Conf. Proc.*, pages 53–82. Amer. Math. Soc., Providence, RI, 2000.

[3] Hui Huang and Manuel Kauers. D-finite numbers, 2016. Preprint available at ArXiv.

[4] Maxim Kontsevich and Don Zagier. Periods. In *Mathematics unlimited—2001 and beyond*, pages 771–808. Springer, Berlin, 2001.

[5] Bruno Salvy and Paul Zimmermann. Gfun: a maple package for the manipulation of generating and holonomic functions in one variable. *ACM Transactions on Mathematical Software*, 20(2):163–177, 1994.

[6] Richard P. Stanley. Differentiably finite power series. *European J. Combin.*, 1(2):175–188, 1980.

The category of finite-dimensional representations of periplectic Lie superalgebras

Martina Balagovic[1], Zajj Daugherty[2], Inna Entova-Aizenbud[3], Iva Halacheva[4], Johanna Hennig[5], Mee Seong Im[6], Gail Letzter[7], Emily Norton[8], Vera Serganova[9], and Catharina Stroppel[10]

[1] *School of Mathematics and Statistics, Newcastle University, Newcastle upon Tyne NE1 7RU UK, martina.balagovic@newcastle.ac.uk*
[2] *Department of Mathematics, City College of New York, New York, NY 10031 USA, zdaugherty@gmail.com*
[3] *Department of Mathematics, Tel Aviv University, Tel Aviv, Israel, inna.entova@gmail.com*
[4] *Department of Mathematics and Statistics, Lancaster University, Lancaster, LA1 4YF UK, i.halacheva@lancaster.ac.uk*
[5] *Department of Mathematical and Statistical Sciences, University of Alberta, Edmonton, Alberta T6G 2G1 Canada, jhennig1@ualberta.ca*
[6] *Department of Mathematical Sciences, United States Military Academy, West Point, NY 10996 USA, meeseongim@gmail.com*
[7] *Department of Defense, Ft. George G. Meade, MD 20755 USA, gletzter@verizon.net*
[8] *Max Planck Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany, enorton@mpim-bonn.mpg.de*
[9] *Department of Mathematics, University of California at Berkeley, Berkeley, CA 94720 USA, serganov@math.berkeley.edu*
[10] *Mathematisches Institut, Universitaet Bonn, Endenicher Allee 60, 53115 Bonn, Germany, stroppel@math.uni-bonn.de*

Let $V = V_{\overline{0}} \oplus V_{\overline{1}}$, a $2n$-dimensional $\mathbf{Z}_2$-graded complex vector space, where $\dim V_{\overline{0}} = \dim V_{\overline{1}} = n$. Then the endomorphism algebra $\mathrm{End}(V)$ inherits the structure of a vector superspace $gl(n|n)$ from V.

Now suppose V is equipped with a nondegenerate odd symmetric form on $V \otimes V$ satisfying

$$\beta(v,w) = \beta(w,v) \quad \text{and} \quad \beta(v,w) = 0 \text{ if } \overline{v} = \overline{w}, \tag{1}$$

where $\overline{v}$ is the parity of a homogeneous element $v \in V$. We define the periplectic (or strange) Lie superalgebra $p(n)$ as the set of all $X \in \mathrm{End}(V)$ preserving the bilinear form β, i.e., X satisfies

$$\beta(Xv,w) + (-1)^{\overline{X}\overline{v}}\beta(v,Xw) = 0. \tag{2}$$

With respect to a fixed basis $V_{\overline{0}} = \mathrm{span}_{\mathbf{C}}\{e_1,\dots,e_n\}$ and $V_{\overline{1}} = \mathrm{span}_{\mathbf{C}}\{f_1,\dots,f_n\}$, a periplectic Lie superalgebra is described as

$$p(n) = \left\{ \begin{pmatrix} A & B \\ C & -A^t \end{pmatrix} : B = B^t, C = -C^t \right\}.$$

I will introduce the representation theory of periplectic Lie superalgebras by providing the combinatorics of the category and its underlying highest weight structure, and I will discuss weight diagrams, which are a useful combinatorial tool, allowing us to compute the multiplicities of standard modules in indecomposable projective modules and of simple modules in standard modules.

More precisely, translation functors on the category $\mathscr{F}_n$ of finite-dimensional representations of $p(n)$ using the endomorphism of the endofunctor $-\otimes V$ will be defined. I will then define the actions of translation functors on thick and thin Kac modules, which categorically lift the Temperley-Lieb relations associated to the infinite symmetric group. Next, I will define the notion of weight diagrams for dominant weights and explain the associated combinatorics of the actions of translation functors on standard and costandard objects in terms of the diagrams. This involves moving a shaded ball left or right, depending on the translation functor and the weight. I will also explain the duality for simple modules in terms of weight diagrams.

Finally, we define the minimal equivalence relation on the set of dominant weights λ and μ such that $\lambda \sim \mu$ if μ is obtained from λ by sliding a shaded ball in a certain way. This implies that simple modules $L(\lambda)$ and $L(\mu)$ belong to the same block if and only if $\lambda \sim \mu$. I will give a classification of the blocks in $\mathscr{F}_n$ and describe the action of translation functors on these blocks.

References

[1] M. Balagovic, Z. Daugherty, I. Entova-Aizenbud, I. Halacheva, J. Hennig, M. Im, G. Letzter, E. Norton, V. Serganova, and C. Stroppel, *Translation functors and decomposition numbers for the periplectic Lie superalgebra $p(n)$,* submitted, arXiv:1610.08470.

Bernoulli symbol on multiple zeta values at negative integers

Lin Jiu[1], Victor H. Moll[2], Christophe Vignat[3]

[1] *RICAM, Austrian Academy of Sciences, Linz, Austria, lin.jiu@ricam.oeaw.ac.at*
[2] *Tulane University, New Orleans, U. S. A., vhm@tulane.edu*
[3] *LSS/Supelec, Université Paris Sud Orsay, Paris, France cvignat@tulane.edu*

The multiple zeta functions are defined by, for $\{n_i\}_{i=1}^r \subset \mathbb{C}$

$$\zeta_r(n_1,\ldots,n_r) = \sum_{0<k_1<\cdots<k_r} \frac{1}{k_1^{n_1}\cdots k_r^{n_r}}, \tag{1}$$

provided that $\sum_{j=1}^k \mathrm{Re}(n_{r+1-j}) > k$, $1 \le k \le r$ ([2, S3]). Values at integer points $\mathbf{n} = (n_1,\ldots,n_r)$ satisfying the constraints are called *multiple zeta values* (MZV). Zhao [4] showed that (1) has an analytic continuation to $\mathbb{C}^r$, not uniquely, due to the *Hartogs' phenomenon*. Thus, several authors have proposed different approaches. For example, Sadaoui [3] used *Raabe's identity* to compute the values.

Theorem 1. *(Sadaoui) [3, eq. (4.10)]*

$$\zeta_r(-n_1,\ldots,-n_r) = \frac{(-1)^r}{n_r+1} \sum_{k_2,\ldots,k_r} \frac{\prod_{j=2}^r \mathfrak{A}\left(\sum_{i=j}^r (n_i+r-j+1) - \sum_{i=j+1}^r k_i \,\middle|\, k_j\right)}{\left(\bar{n}+r-\bar{k}\right)} \times \sum_{l_1,\ldots,l_r} \binom{\bar{n}+r-\bar{k}}{l_1}\binom{k_2}{l_2}\cdots\binom{k_r}{l_r} B_{l_1}\cdots B_{l_r},$$

where $k_2,\ldots,k_r \ge 0$, $l_j \le k_j$ for $2 \le j \le r$ and $l_1 \le \bar{n}+r+\bar{k}$ with $\bar{n} = \sum_{j=1}^r n_j$, $\bar{k} = \sum_{j=2}^r k_j$, $\mathfrak{A}(t|s) := \binom{t}{s}/t$, and B_n is the n^{th} Bernoulli number.

On the other hand, Akiyama and Tanigawa [1] used the Euler-MacLaurin summation formula to obtain results, one of which is the following recurrence. (Here, the notation $\bar{\zeta}$ instead of ζ is used to distinguish two continuations.)

Theorem 2. *(Akiyama and Tanigawa) [1, eq. (15)]*

$$\begin{aligned}\bar{\zeta}_r(-n_1,\ldots,-n_r) = &-\bar{\zeta}_{r-1}(-n_1,\ldots,-n_{r-2},-n_{r-1}-n_r-1)/(n_r+1)\\ &-\bar{\zeta}_{r-1}(-n_1,\ldots,-n_{r-2},-n_{r-1}-n_r)/2\\ &+\sum_{q=1}^{n_r}(-n_r)_q a_q \bar{\zeta}_{r-1}(-n_1,\ldots,-n_{r-2},-n_{r-1}-n_r+q),\end{aligned}$$

where $(-n_r)_q = (-n_r)(-n_r+1)\cdots(-n_r+q-1)$ and $a_q := B_{q+1}/(q+1)!$.

We generalized the idea of Bernoulli symbol to the following $\mathcal{C}$ symbols.

Definition 1. $\mathcal{C}_{1,2,\ldots,k}$ is defined recursively via Bernoulli symbols $\mathcal{B}_1,\ldots,\mathcal{B}_r$ as

$$\mathcal{C}_1^n=\frac{\mathcal{B}_1^n}{n},\ \mathcal{C}_{1,2}^n=\frac{(\mathcal{C}_1+\mathcal{B}_2)^n}{n},\ldots,\ \mathcal{C}_{1,2,\ldots,k+1}^n=\frac{(\mathcal{C}_{1,2,\ldots,k}+\mathcal{B}_{k+1})^n}{n}.$$

Each symbol $\mathcal{C}_{1,2,\ldots,k}$ should be expanded only involving $\mathcal{B}_k$, and then:

1. each power $\mathcal{B}_k^p$ should be evaluated as $\mathcal{B}_k^p\to B_p$;
2. if $k\neq l$, product $\mathcal{B}_k^p\mathcal{B}_l^q$ is evaluated as $\mathcal{B}_k^p\mathcal{B}_l^q\to B_pB_q$.

Theorem 3. *(L. Jiu, V. H. Moll, and C. Vignat)*

$$\zeta_r(-n_1,\ldots,-n_r)=\prod_{k=1}^{r}(-1)^{n_k}\mathcal{C}_{1,\ldots,k}^{n_k+1}=\bar{\zeta}_r(-n_1,\ldots,-n_r).$$

Not only do we obtain a symbolic, more compact, effective expression leading to further results such as (denote $\mathbf{a}_k=(a_1,\ldots,a_k)$ for $\mathbf{a}=(a_1,\ldots,a_r)$ and $k<r$)
• recursion formula

$$\zeta_r(-\mathbf{n};\mathbf{z})=\frac{(-1)^{n_r}}{n_r+1}\sum_{l=0}^{n_r+1}\binom{n_r+1}{l}(-1)^l\,\zeta_{r-1}(-\mathbf{n}_{r-2},-n_{r-1}-l;\mathbf{z})\,B_{n_r+1-l}(z_r);$$

• contiguity identity: for $\mathcal{Z}_r^l=\zeta_r(-\mathbf{n}_{r-1},-n_r-l;\mathbf{z})$;

$$\zeta_r(-\mathbf{n};\mathbf{z}_{r-1},z_r+1)=\zeta_r(-\mathbf{n};\mathbf{z}_{r-1},z_r)+(-1)^{n_r}(z_r-\mathcal{Z}_{r-1})^{n_r};$$

• and generating function

$$\begin{aligned}F_r(w_1,\ldots,w_r)&:=\sum_{n_1,\ldots,n_r\geq 0}\frac{w_1^{n_1}\cdots w_r^{n_r}}{n_1!\cdots n_r!}\zeta_r(-n_1,\ldots,-n_r)\\&=\big(F_1(w_r,-\partial_{r-1})\cdots F_1(w_2,-\partial_1)\big)\bullet F_1(w_1,0),\end{aligned}$$

where $\partial_i=\partial/\partial w_i$ and $F_1(w,z)=\frac{e^{-wz}}{e^{-w}-1}-\frac{1}{w}$, but also it surprisingly reveals that both analytic continuations in Theorem 1 and Theorem 2 coincide. An explanation of such phenomena is part of future work.

References

[1] S. Akiyama and Y. Tanigawa, *Multiple zeta values at non-positive integers*, Ramanujan J. **5**, pp. 327–351 (2001).

[2] K. Matsumoto, *On the analytic continuation of various multiple zeta functions*, in *Number Theory for the Millennium*, vol. II. Bennett, M. A. et al (eds.), A. K. Peters, Natick, MA, pp. 417–440 (2002).

[3] B. Sadaoui, *Multiple zeta values at the non-positive integers*, C. R. Acad. Sci. Paris, Ser. 1, **12**, pp. 977–984 (2014).

[4] J. Zhao, *Analytic continuation of multiple zeta-functions*, Proc. Am. Math. Soc. **128**, pp. 1275–1283 (2000).

Bounds for D-Finite Substitution

Manuel Kauers[1], Gleb Pogudin[1]

[1] *Institute for Algebra, Johannes Kepler University Linz, Austria,*
{manuel.kauers,gleb.pogudin}@jku.at

A function f is called D-finite if it satisfies a linear differential equation with polynomial coefficients,

$$p_0(x)f(x) + p_1(x)f'(x) + \cdots + p_r(x)f^{(r)}(x) = 0.$$

Typical examples include e^x, $\log(x)$, as well as non-elementary functions such as Bessel functions or the Error function. A function g is called algebraic if it satisfies a polynomial equation,

$$q_0(x) + q_1(x)g(x) + \cdots + p_s(x)g(x)^s = 0.$$

Typical examples include $\sqrt{x}$ or $\sqrt[3]{5x^2-3} + 28x^9$.

It is well-known that every algebraic function is D-finite, and that, more generally, whenever f is D-finite and g is algebraic, then the composition $g \circ f$ is again D-finite. Algorithms for computing a linear differential equation for $g \circ f$ from a given linear differential equation for f and a given polynomial equation for g are part of the standard repertoire of software packages for D-finite functions.

We consider the question how big an equation for $g \circ f$ will be in dependence of the sizes of the equations of f and g. In a first approach, we use a standard argument based on linear algebra: we set up a linear system over the constant field and balance the number of variables and equations. This leads to a so-called order-degree curve, a curve in $\mathbb{R}^2$ such that for all points $(r,d) \in \mathbb{N}^2$ above the curve, there exists an equation for $g \circ f$ of order r with polynomial coefficients of degree at most d.

The order-degree curve obtained in this way is far from tight. In a second approach, we derive a formula for an order-degree curve by analyzing the singularities of the resulting operator. This requires some work because these singularities are not directly accessible from the given data for f and g. However, the work pays off because the resulting curve turns out to be extremely tight, at least generically. We will show some examples during the talk.

Formulas for the resulting curves as well as full details of our derivations can be found in the preprint [1].

References

[1] M. Kauers and G. Pogudin, *Bounds for D-finite Substitution*, ArXiv 1701.07802, Jan 2017.

Algorithmic Aspects of the Černý Conjecture

Andrzej Kisielewicz

University of Wrocław, Wrocław, Poland, andrzej.kisielewicz@math.uni.wroc.pl

In this talk we present the use of computer search and the role of algorithms in attempts to solve the Černý Conjecture, which is one of the most longstanding open problems in automata theory.

We deal with finite deterministic automata $A = (Q, \Sigma, \delta)$, where Q is a finite set of the states, Σ is a finite input alphabet, and $\delta : Q \times \Sigma \to Q$ is the transition function defining the action of the letters in Σ on Q. The action extends in the natural way to the action of words over Σ on Q and is denoted simply by $qw = \delta(q, w)$.

An automaton A is *synchronizing* if there exist a word w over Σ and a state $q_0 \in Q$ such that for each state $q \in Q$ the image $qw = q_0$. In other words, the word w brings the automaton A to the state q_0 with no regard to in what state it happens to be. Such a word w, if exists, is called a *reset* word for A.

The Černý conjecture states that if an automaton A with n states is synchronizing, then it has a reset word of length not exceeding $(n-1)^2$. It has been proved in many particular cases, but in general, is still open. The best general bound achieved so far for the shortest reset word in synchronizing automata is $(n^3 - n)/6$. The most general result proving the conjecture for a class of automata has been obtained in [2]. (See also [7] for an excellent survey of the topic).

We present our two recent results on the Černý conjecture involving an extensive use of computers and dedicated algorithms. The first concerns the verification of the conjecture for small automata. In [1] all binary automata (that is, those with a two-element alphabet) having at most $n = 9$ states have been checked. Note that there are 9^{18} labeled binary automata with $n = 9$ states, so some more sophisticated approach than *brute force* must be applied. In [1], the authors have managed to restrict the search to the class of the so-called *initially connected* automata. Earlier, the checking of all automata with at most $n = 10$ states was reported in [5], yet no details of computation have been described.

In [4], using a dedicated algorithm for parallel computation, we have verified the conjecture for all binary automata with $n \leq 12$ states. The case of automata with $n = 12$ states took about 100 years of computation time of a single processor core. The number of automata generated by our algorithm in this case was about 10^{15}, which should be compared with about 2.2×10^{17} of non-isomorphic initially connected automata (that one would need to generate applying the technique described in [1]), and 12^{24} of all binary automata with $n = 12$ states.

In [2], the conjecture is considered in terminology of colored digraphs, which refers to the famous Road Coloring problem [6]. We consider edge-colored digraphs with the property that no two edges leaving a vertex have a common color. Such an assignment of colors to edges is called a *road coloring*. Then, given a vertex x, each finite sequence of colors $\alpha_1, \ldots, \alpha_m$ (repetitions allowed) may be considered as a description of a path (road) starting in x and leading to a uniquely determined vertex $y \in V$. (Absence of an edge of a given color α leaving a given vertex x is interpreted as a loop at x colored α).

We are interested in "universal instructions" making it possible to reach a fixed vertex y with no regard at which vertex we start. A sequence of colors $\alpha_1, \ldots, \alpha_m$ such that for each vertex x it describes a path from x to the given y is called a *synchronizing* sequence (for the vertex y).

We define a class of colored digraphs, having a relatively small number of junctions between paths determined by different colors, and prove that the automata corresponding to the digraphs in this class satisfy the Černý conjecture. From computational point of view, we present a number of algorithms finding short synchronizing sequences for various types of graphs. We show that in spite of that the class is defined in a uniform way and the digraphs in the class seem very similar, it requires to apply very different types of algorithms to find a synchronizing sequence short enough.

This suggests that the difficulty in proving the Černý conjecture in its generality may lie in that the solution consists of a large collection of very different algorithmic ideas covering the whole spectrum of synchronizing automata.

References

[1] D. S. Ananichev, M. V. Volkov, and V. V. Gusev. *Primitive digraphs with large exponents and slowly synchronizing automata*, J. Math. Sci. 192, pp. 263–278 (2013).

[2] M. Grech, A Kisielewicz *The Černý conjecture for automata respecting intervals of a directed graph*, Discrete Math. Theoretical Comput. Sci. 15, pp. 61-72 (2013).

[3] M. Grech, A. Kisielewicz *Synchronizing sequences for road colored digraphs*, to appear.

[4] A. Kisielewicz, J. Kowalski, M. Szykuła, *Experiments with Synchronizing Automata*, CIAA 2016, LNCS 9705, pp. 176-188 (2016).

[5] A. N. Trahtman, *An efficient algorithm finds noticeable trends and examples concerning the Černý conjecture*, in Mathematical Foundations of Computer Science, LNCS 4162, pp. 789–800 (2006).

[6] A. N. Trahtman, *The road coloring problem*, Israel J. Math. 172, pp, 51–60 (2009).

[7] M. V. Volkov. *Synchronizing automata and the Černý conjecture*, LATA 2008, LNCS 5196, pp. 11–27 (2008).

Algorithms and open problems for weighing matrices

Ilias S. Kotsireas[1]

[1] *Wilfrid Laurier University, Waterloo, Canada, ikotsire@wlu.ca*

Weighing matrices are generalizations of Hadamard matrices, that arise in constructive and algorithmic combinatorics and have applications in Coding Theory, Cryptography, Quantum Computing and other areas. The concepts of periodic and aperiodic autocorrelation can be used to provide a succinct and unified description of several different classes of combinatorial matrices [1], including weighing matrices of special structure. We will survey some algorithms to construct such weighing matrices, with emphasis on their computer algebra, data analytics, big data and parallel computing aspects. We will also mention some conjectures and open problems.

References

[1] I. Kotsireas. Algorithms and Meta-heuristics for Combinatorial Matrices. Handbook of Combinatorial Optimization, 2nd Edition, 2013, Panos Pardalos, Ding-Zhu Du, Ronald Graham (Editors) pp 283–309.

Wilf classification of subsets of four-letter patterns

Toufik Mansour[1]

[1] *Department of Mathematics, University of Haifa, 3498838 Haifa, Israel, tmansour@univ.haifa.ac.il*

In the last decades, the problem of avoiding patterns in different combinatorial structures like permutations, coloured permutations, compositions, partitions, set partitions, etc. has been studied by many authors from many different point of views. In this talk, we restrict to permutations and the problem of pattern avoidance for them.

Let $\mathcal{S}_n$ be the symmetric group of all permutations of $[n] \equiv \{1,\ldots,n\}$. Let $\pi = \pi_1\pi_2\cdots\pi_n \in \mathcal{S}_n$ and $\tau = \tau_1\tau_2\cdots\tau_k \in \mathcal{S}_k$ be two permutations. We say that π *contains* τ if there exists a subsequence $1 \le i_1 < i_2 < \cdots < i_k \le n$ such that $\pi_{i_1}\pi_{i_2}\cdots\pi_{i_k}$ is *order-isomorphic* to τ, that is, $\pi_{i_a} < \pi_{i_b}$ if and only if $\tau_a < \tau_b$; in such a context τ is usually called a *pattern*. For example, $\pi = 35412$ contains the pattern $\tau = 231$. We say that π *avoids* τ, or is τ*-avoiding*, if such a subsequence does not exist. For example, 35412 avoids 123. The set of all τ-avoiding permutations in $\mathcal{S}_n$ is denoted by $\mathcal{S}_n(\tau)$. For an arbitrary finite collection of patterns T, we say that π *avoids* T if π avoids every pattern τ in T; the corresponding subset of $\mathcal{S}_n$ is denoted by $\mathcal{S}_n(T)$, i.e., $\mathcal{S}_n(T) = \bigcap_{\tau\in T}\mathcal{S}_n(\tau)$. The sets of patterns T and T' belong to the same *Wilf class* (or are *Wilf-equivalent*) if and only if $|\mathcal{S}_n(T)| = |\mathcal{S}_n(T')|$ for all $n \ge 0$.

In 1985, Simion and Schmidt found the cardinality of $\mathcal{S}_n(T)$, where $T \subseteq \mathcal{S}_3$. Thus, the case of patterns of length three is well-known. Let us turn to patterns of length four. For this case, much less is known and is seems hopeless to get an explicit formula for $|\mathcal{S}_n(T)|$ where $T \subseteq \mathcal{S}_4$ is arbitrary. Already the case of avoiding exactly one pattern $\tau \in \mathcal{S}_4$ is not trivial. It was shown that there are three essentially different cases, namely $\mathcal{S}_n(\tau)$ where $\tau \in \{1342, 1234, 1324\}$. Since $|\mathcal{S}_7(1342)| = 2740$, $|\mathcal{S}_7(1234)| = 2761$ and $|\mathcal{S}_7(1324)| = 2762$, these three patterns comprise three different Wilf classes. If we denote the number of symmetry classes and Wilf classes of subsets of k patterns in $\mathcal{S}_4$ by s_k and w_k, respectively, then this means that $w_1 = 3$.

Let us turn to subsets $T = \{\tau_1, \tau_2\}$ with exactly two patterns in $\mathcal{S}_4$. There do exist $\binom{24}{2} = 276$ such subsets T. Le established that these 276 subsets form 38 distinct Wilf classes, i.e., $w_2 = 38$. It seems that the case of k with $3 \le k \le 23$ has not been studied in the literature before the recent work of Mansour and Schork.

Thus, the aim of this talk is discuss how to determine w_k for $3 \leq k \leq 24$. Since the number of subsets of $\mathcal{S}_4$ containing at least 3 patterns is given by $\sum_{k=3}^{24} \binom{24}{k} = 16776915$, it seems to be impossible to reach by constructing explicit bijections between sets of permutations. The way out is to combine several software programs to do the work for us!!

This talk based on recent works of the author with David Callan, Mark Shattuck and Matthias Schork.

Automatic proofs for establishing the structure of integer sequences avoiding a pattern

Lara Pudwell[1], Eric Rowland[2]

[1] *Valparaiso University, Valparaiso, Indiana, USA*
[2] *Hofstra University, Hempstead, New York, USA, eric.rowland@hofstra.edu*

Is there an infinite sequence on the alphabet $\{0,1,2\}$ containing no block that occurs twice consecutively? Questions like this were investigated a century ago by the Norwegian mathematician Axel Thue, who produced some of the earliest results in combinatorics on words. If a pattern is avoidable on a given alphabet, it is natural to ask about the lexicographically least sequence that avoids the pattern. Occasionally the structure of this sequence can be discovered and proved by hand. But for many patterns this sequence is sufficiently complex that computer-assisted discovery, followed by automated proofs, seems to be necessary to make any progress.

Here we are interested in the lexicographically least integer sequence avoiding a given fractional power. Let a and b be relatively prime positive integers with $\frac{a}{b} > 1$. We say that a word w is an $\frac{a}{b}$*-power* if w can be written $v^e x$ where e is a non-negative integer, x is a prefix of v, and $|w|/|v| = a/b$. For example, $011101 = (0111)^{3/2}$ is a $\frac{3}{2}$-power. A sequence is $\frac{a}{b}$*-power-free* if none of its nonempty factors are $\frac{a}{b}$-powers. Avoiding $\frac{3}{2}$-powers, for example, means avoiding factors xyx where $|x| = |y| \geq 1$.

Notation. Let $\mathbf{s}_{a/b}$ denote the lexicographically least $\frac{a}{b}$-power-free infinite sequence on the alphabet $\mathbb{Z}_{\geq 0}$.

Guay-Paquet and Shallit [2] described the structure of the lexicographically least square-free sequence

$$\mathbf{s}_2 = 0102010301020104010201030102010 5\cdots.$$

More generally, for an integer $a \geq 2$ we have $\mathbf{s}_a = \varphi^\infty(0)$, where $\varphi : \mathbb{Z}_{\geq 0}^* \to \mathbb{Z}_{\geq 0}^*$ is the morphism defined by $\varphi(n) = 0^{a-1}(n+1)$. Rowland and Shallit [4] gave a recurrence for

$$\mathbf{s}_{3/2} = 001102\,100112\,001103\,100113\,001102\,100114\,001103\,100112\cdots.$$

The sequence $\mathbf{s}_{3/2}$ is 6-regular in the sense of Allouche and Shallit [1]; informally, this means that the ith term can be computed directly from the base-6 digits of i.

Significant motivation for the present study is to put this '6' into context by studying $\mathbf{s}_{a/b}$ systematically. We show that for many rational numbers $\frac{a}{b}$, the sequence $\mathbf{s}_{a/b}$ is the fixed point of a k-uniform morphism for some integer k. (A morphism φ on an alphabet Σ is *k-uniform* if $|\varphi(n)| = k$ for all $n \in \Sigma$.)

For example, consider

$$\mathbf{s}_{5/3} = 0000101\,0000101\,0000101\,0000101\,0000102\,0000101\,0000102\cdots.$$

This sequence belongs to an infinite family of sequences, all generated by similar morphisms.

Theorem. *Let a,b be relatively prime positive integers such that $\frac{5}{3} \leq \frac{a}{b} < 2$ and $\gcd(b,2) = 1$. Let φ be the $(2a-b)$-uniform morphism defined by*

$$\varphi(n) = 0^{a-1}\,1\,0^{a-b-1}\,(n+1)$$

for all $n \in \mathbb{Z}_{\geq 0}$. Then $\mathbf{s}_{a/b} = \varphi^{\infty}(0)$.

There are two steps in the proof of this theorem. The first step is to verify that the morphism φ is *$\frac{a}{b}$-power-free* (that is, $\varphi(w)$ is $\frac{a}{b}$-power-free whenever w is $\frac{a}{b}$-power-free). The second step is to verify that φ is *lexicographically least* with respect to $\frac{a}{b}$ (that is, if w is $\frac{a}{b}$-power-free and decrementing any term introduces an $\frac{a}{b}$-power, then decrementing any term in $\varphi(w)$ introduces an $\frac{a}{b}$-power ending at that position). Since the word 0 is $\frac{a}{b}$-power-free and lexicographically least of its length, if φ is an $\frac{a}{b}$-power-free, lexicographically least morphism then $\mathbf{s}_{a/b} = \varphi^{\infty}(0)$. For details, see [3].

We use software to carry out these steps, establishing the structure of several families of sequences $\mathbf{s}_{a/b}$. As a consequence, it follows that these sequences are k-regular for various values of k depending on $\frac{a}{b}$. This suggests the following main question.

Open question. For which rational numbers $\frac{a}{b} > 1$ does there exist an integer k such that $\mathbf{s}_{a/b}$ is k-regular?

References

[1] Jean-Paul Allouche and Jeffrey Shallit, The ring of k-regular sequences, *Theoretical Computer Science* **98** (1992) 163–197.

[2] Mathieu Guay-Paquet and Jeffrey Shallit, Avoiding squares and overlaps over the natural numbers, *Discrete Mathematics* **309** (2009) 6245–6254.

[3] Lara Pudwell and Eric Rowland, Avoiding fractional powers over the natural numbers, `https://arxiv.org/abs/1510.02807`.

[4] Eric Rowland and Jeffrey Shallit, Avoiding $3/2$-powers over the natural numbers, *Discrete Mathematics* **312** (2012) 1282–1288.

External Littelmann paths for crystals of Type A

Ola Amara-Omari[1], Malka Schaps[2]

[1] *Supported by Ministry of Science, Technology and Space fellowship , at Bar-Ilan University, Ramat-Gan, Israel olaomari77@hotmail.com*

[2] *Bar-Ilan University, Ramat-Gan, Israel, mschaps@macs.biu.ac.il*

Affine Lie algebras of type A and their highest weight representations are important in physics. They correspond to the symmetric group, the most important of the reflection groups. The basis elements of a highest weight representation with highest weight Λ of level r, organized into a Kashiwara crystal, correspond to the simple modules of the cyclotomic Hecke algebras of weight Λ and have three combinatorial representations: as multipartitions, as Littelmann paths and as canonical basis elements.

We wrote a computer program in Sage which calculated all three of these combinatorial representations simultaneously for the beginning degrees of a Kashiwara crystal. The program slows down at around degree 16, so most of our examples are in the range up to 16. We began with the case of rank $e = 2$, for which the multipartitions corresponding to basis elements, called the e-regular multipartions, are completely understood by work of Mathas [M]. We succeeded in finding a direct connection between the multipartitions at the corners of the Kashiwara crystal, which we called extremal, and Littelmann paths of a type we call standard.

Following Mathas, we write

$$\Lambda = a\Lambda_0 + b\Lambda_1. \tag{1}$$

We started with the easy case $r = 1$, and by constructing an object called the block-reduced crystal graph [AS], discovered that the corner points were alternating, i.e., had odd and even length rows alternating. Defining segment boundaries when the differences were more than one, we were able to find a representation of the external Littelmann paths which depended on the length of the first row of the segment and the distance to the top of the partitions.

A Littelman path [L] is a piecewise linear path from the unit interval to the weight space, represented in the computer by a sequence of vectors called defect 0 weights, together with coefficients which are rational numbers and determine the endpoints of the piecewise linear subpaths of the Littelmann path. The first and last vectors are called the ceiling and the floor [AKT]. We were able to show that there were no gaps between the ceiling and the floor and give exact formulae for the coefficients. For a segment i, we let b_i be the distance from the top of the partition to the bottom of the segment, and let n_i' be the number we would get if the top row

of the segment is continued up in a triangular fashion to the top row. Then we get parameter boundaries $\frac{b_i}{m}$ for m with $n'_i \geq m > n'_{i+1}$. The paths had an interesting structure: long paths where the segments were being widened, and short oscillating paths where the segments were being deepened.

We then turned to the case of $r > 1$, which was considerably more challenging. However, we were helped along by the intuition we had gained from working with the $r = 1$ case. We again divided the multipartition into segments, but now a segment could contain more than one subpartition. We replaced the alternating condition with a condition we called "residue homogeneous", which ensured that the end points of all the rows would have the same residue 0 or 1. We no longer had a simple, gapless Littelmann path between ceiling and floor. To deal with this situation, we defined a multipartition which we called a pseudo-floor, which was a defect 0 partition truncated by replacing some of the subpartitions by the emply partition. We believe this object to be new.

The induction for the $r >1$ case started by constructing the Littelmann path for the pseudo-floor of the highest segment and began adding segments going downward. The resulting Littelmann paths, projected onto the hubs, looked very similar to the paths we had found for the $r = 1$ case, except that the end was quirky because of the pseudo-floor.

Finally, the rational numbers which gave the boundaries for the parametrization were also more complicated. Each was of the form

$$e_m = \frac{c_m}{d_m}, \tag{2}$$

where d_m was the number of nodes added to a defect 0 multipartion with first row $m-1$ to get that for m. Similarly c_m is the number of nodes added to widen the segment. Standard Littelmann paths have parameter boundaries in this form and are quite common, as we found from our experimental work on the case $e = 3$. In the general case they usually had gaps, which occurred when $e_m = e_{m+1}$. There is no known non-recursive criterion for e-regular multipartitions for $e = 3$ and level $r > 3$. We are hoping to get results in this direction for the external basis elements.

References

[AKT] S. Ariki, V. Kreiman, & S. Tsuchioka, *On the tensor product of two basic represenations of* $U_v(\hat{sl}_e)$, Advances in Mathematics 218 (2008), 28-86.

[AS] H. Arisha & M. Schaps *Maximal Strings in the crystal graph of spin representations of symmetric and alternating groups*, Comm. in Alg. (2009).

[L] P. Littelmann, *Paths and root operators in representation theory*, Annals of Mathematics, 2nd Ser. Vol. 142, No. e (Nov., 1995), 499-525.

[M] A. Mathas, *Simple modules of Ariki-Koike algebras*,Proc. Sym. Pure Math(1997), 383-396.

Time for the New Ansatz (?)

Thotsaporn Thanatipanonda[1]

[1] *Mahidol University International College, {thotsaporn}@gmail.com*

Mathematics is a science of describing patterns. It is a commonly known technique to describe the patterns of sequences using recurrence relations, both by using constant coefficients (aka C-finite ansatz, [1, 4]) i.e. the sequence $\{a(n)\}_{n=0}^{\infty}$ where there are constants $c_0, c_1, \ldots, c_{k-2}, c_{k-1}$ such that

$$c_0 a(n) + c_1 a(n+1) + \cdots + c_{k-1} a(n+k-1) + a(n+k) = 0, \quad \text{for all } n \geq 0,$$

or by using polynomial coefficients (aka holonomic ansatz, [1, 3]) i.e. the sequence $\{b(n)\}_{n=0}^{\infty}$ where there are polynomials $p_0(n), p_1(n), p_2(n), \ldots, p_{k-1}(n), p_k(n)$ with $p_k(n) \neq 0$, such that

$$p_0(n) b(n) + p_1(n) b(n+1) + \cdots + p_k(n) b(n+k) = 0, \quad \text{for all } n \geq 0.$$

However there are still many important sequences that do not belong to these classes. The first example is the (Somos) sequence defined by a complicated looking non-linear recurrence relation:

$$a(n)(a(n+1)\cdot a(n+3) - a(n+2)^2) - a(n+2)\cdot a(n+1)^2 = 0, \quad \text{for all } n \geq 0$$

where $a(0) = 1, a(1) = 1$ and $a(2) = 2$.

Here are the first ten terms of the sequence:

$$1, 1, 2, 6, 30, 240, 3120, 65520, 2227680, 122522400$$

This sequence is growing too fast to be C-finite or holonomic, but still simple enough for a human to detect the pattern. This strongly suggests us to create a new ansatz for this type of sequences.

The second example came up when I worked on Schmidt's number, [2]. This is part of the main theorem. For $k \geq 0$ and $r \geq 1$, define $a_{k,j}^{(r)}$ as follows:

$$\binom{n}{k}^r \binom{n+k}{k}^r = \sum_j a_{k,j}^{(r)} \binom{n}{j} \binom{n+j}{j}.$$

It is not clear at all that this multi-dimensional sequence $a_{k,j}^{(r)}$ are integers until we discover the non-holonomic recurrence relation of $a_{k,j}^{(r)}$:

$a_{k,k}^{(1)} = 1$, $a_{k,j}^{(1)} = 0$ $(j \neq k)$ and

$$a_{k,j}^{(r+1)} = \sum_i \binom{k+i}{i} \binom{k}{j-i} \binom{j}{k} a_{k,i}^{(r)}.$$

In conclusion, we will explore many of these examples and propose some new types of ansatz accordingly.

References

[1] Manuel Kauers and Peter Paule, *The Concrete Tetrahedron*, Springer, 2011.

[2] Thotsaporn Thanatipanonda, *A Simple Proof of Schmidt's Conjecture*, Journal of Difference Equations and Applications, 20(3), pp. 413-415 (2014).

[3] Doron Zeilberger, *The HOLONOMIC ANSATZ II. Automatic DISCOVERY(!) and PROOF(!!) of Holonomic Determinant Evaluations*, Annals of Combinatorics, 11, pp. 241-247 (2007).

[4] Doron Zeilberger, *The C-finite ansatz*, The Ramanujan Journal, 31(1), pp. 23-32 (2013).

[5] Shalosh B. Ekhad and Doron Zeilberger, *How To Generate As Many Somos-Like Miracles as You Wish*, Journal of Difference Equations and Applications, 20, pp. 852-858 (2014).

Computer Algebra Algorithms for Proving Jacobi Theta Function Identities

Liangjie Ye[1]

[1] *RISC, Johannes Kepler University, Austria, liangjie.ye@risc.jku.at*

Many number theorists, e.g., Ramanujan, Hardy, Rademacher, Berndt, Borwein, etc., have proved a substantial amount of theta function relations by hand (see [1]–[8]). There was no general method for proving such relations, and the computation in their proofs are usually tedious.

Example 1. *[7, (93.22)]*

$$\theta_3^{(4)}(0|\tau)\theta_3(0|\tau) - 3(\theta_3''(0|\tau))^2 - 2\theta_3(0|\tau)^2\theta_2(0|\tau)^4\theta_4(0|\tau)^4 \equiv {}^1 0.$$

Example 2. *[5, p. 17]*

$$\sum_{j=1}^{4} \theta_j(x|\tau)\theta_j(y|\tau)\theta_j(u|\tau)\theta_j(v|\tau) - 2\theta_3(x_1|\tau)\theta_3(y_1|\tau)\theta_3(u_1|\tau)\theta_3(v_1|\tau) \equiv 0,$$

where $x_1 := \frac{1}{2}(x+y+u+v)$ *and* $y_1 := \frac{1}{2}(x+y-u-v)$, $u_1 := \frac{1}{2}(x-y+u-v)$ *and* $v_1 := \frac{1}{2}(x-y-u+v)$.

Example 3. *[3, p. 218] A form of the cubic modular equation is*

$$\theta_3(0|\tau)\theta_3(0|3\tau) - \theta_4(0|\tau)\theta_4(0|3\tau) - \theta_2(0|\tau)\theta_2(0|3\tau) \equiv 0.$$

Example 4. *[1, p. 285] Let* $\eta(\tau) := e^{\pi i\tau/12}\prod_{k=1}^{\infty}(1-e^{2\pi i\tau k})$. *Then*

$$\theta_3(0|\tau)^2\theta_3(0|5\tau)^2 - \theta_2(0|\tau)^2\theta_2(0|5\tau)^2 - \theta_4(0|\tau)^2\theta_4(0|5\tau)^2 \equiv 8\eta(2\tau)^2\eta(10\tau)^2.$$

By using such theta function relations, several important results can be obtained. For instance, by using Example 1, Rademacher derived the formula for the number of presentations of a natural number as a sum of 10 squares. Moreover, those types of relations also play an important role in physics and in the evaluation of π.

[1] We use the notation $f_1(z_1,z_2,\dots) \equiv f_2(z_1,z_2,\dots)$ if we want to emphasize that the equality between the functions holds for all possible choices of the arguments z_j.

Our goal is to automatize the proving procedures of relations and the discovery of relations. As a first step, in [9] we provided an algorithm to prove identities involving

$$\theta_j^{(k)}(0|\tau) := \frac{\partial^k \theta_j}{\partial z^k}(z|\tau)\bigg|_{z=0}, \quad k \in \mathbb{N} := \{0,1,2,\dots\}.$$

Then, in [10], we extend the function space in [9] and provided two algorithms to prove identities in the form of

$$\sum c(i_1,i_2,i_3,i_4)\theta_1(z|\tau)^{i_1}\theta_2(z|\tau)^{i_2}\theta_3(z|\tau)^{i_3}\theta_4(z|\tau)^{i_4} \equiv 0$$

with $c(i_1,i_2,i_3,i_4) \in \mathbb{K}[\Theta]$, where $\mathbb{K}$ is a computable field and

$$\Theta := \left\{\theta_1^{(2k+1)}(0|\tau) : k \in \mathbb{N}\right\} \cup \left\{\theta_j^{(2k)}(0|\tau) : k \in \mathbb{N} \text{ and } j = 2,3,4\right\}.$$

In addition, by our approach, we can also produce two general classes of relations. In this talk we will briefly show the essence of our methods for [9] and [10], which is mainly based on modular form techniques and the theory of elliptic functions. We will also demonstrate our Mathematica package "ThetaFunctions".

References

[1] B. C. Berndt. *Ramanujan's Notebooks Part III*. Springer, New York, 1991.

[2] J. M. Borwein and P. B. Borwein. *Pi and the AGM: A Study in Analytic Number Theory and Computational Complexity*. Wiley, New York, 1987.

[3] G. H. Hardy. *Ramanujan: Twelve Lectures on Subjects Suggested by His Life and Work*. Cambridge University Press, 1940.

[4] D. F. Lawden. *Elliptic Functions and Applications*. Springer, New York, 1989.

[5] D. Mumford. *Tata Lectures on Theta I*, Prog. Math. Vol. 28, Boston Basel Stuttgart: Birkäuser, 1983.

[6] [DLMF] *NIST Digital Library of Mathematical Functions.* `http://dlmf.nist.gov/`, Release 1.0.14 of 2016-12-21. F. W. J. Olver, A. B. Olde Daalhuis, D. W. Lozier, B. I. Schneider, R. F. Boisvert, C. W. Clark, B. R. Miller, and B. V. Saunders, eds.

[7] H. Rademacher. *Topics in Analytic Number Theory*. Springer, New York, 1973.

[8] E. T. Whittaker and G. N. Watson. *A Course of Modern Analysis*. Cambridge University Press, 1927.

[9] L. Ye. A symbolic decision procedure for relations arising among Taylor coefficients of classical Jacobi theta functions. *J. Symbolic Computation*, 82:134–163, 2017.

[10] L. Ye. Elliptic function based algorithms to prove Jacobi theta function relations. *Submitted.* 26 pages.

Apparent Singularities of D-finite Systems

Manuel Kauers[1], Ziming Li[2], Yi Zhang[3]

[1] *Institute for Algebra, Johannes Kepler University Linz, Austria, manuel@kauers.de*
[2] *KLMM, AMSS, Chinese Academy of Sciences, Beijing, China, zmli@mmrc.iss.ac.cn*
[3] *Institute for Algebra, Johannes Kepler University Linz, Austria, zhangy@amss.ac.cn*

A D-finite function is specified by a linear ordinary differential equation with polynomial coefficients and finitely many initial values. Every singularity of a D-finite function will be a root of the coefficient of the highest order derivative appearing in the corresponding differential equation. For instance, x^{-1} is a solution of the equation $xf'(x)+f(x)=0$, and the singularity at the origin is also the root of the polynomial x. However, the converse is not true. For example, the solution space of the differential equation $xf'(x)-4f(x)=0$ is spanned by x^4 as a vector space, but none of those functions has singularity at the origin.

More specifically, for an ordinary equation $p_0(x)f(x)+\cdots+p_r(x)f^{(r)}(x)=0$ with polynomial coefficients $p_1,\ldots,p_r$ and $p_r\neq 0$, the roots of p_r are called the singularities of the equation. A root α of p_r is call *apparent* if the differential equation admits r linearly independent formal power series solutions in $x-\alpha$. Deciding whether a singularity is apparent is therefore the same as checking whether the equation admits a fundamental system of formal power series solutions at this point. This can be done by inspecting the so-called *indicial polynomial* of the equation at α and solving a system of finitely many linear equations. If a singularity α of an ordinary differential is apparent, then we can always construct a second ordinary differential equation whose solution space contains all the solutions of the first equation, and which does not have α as a singularity any more. This process is called *desingularization*.

The purpose of our work is to generalize the facts sketched above to the multivariate setting. Instead of an ODE, we consider systems of PDEs known as D-finite systems. A D-finite system is a finite set of linear homogeneous partial differential equations with polynomial coefficients in several variables, whose solution space is of finite dimension. For such systems, we define the notion of a singularity in terms of the polynomials appearing in them. We show that a point is a singularity of the system unless it admits a basis of power series solutions in which the starting monomials are as small as possible with respect to some term order. Then a singularity is apparent if the system admits a full basis of power series solutions, the starting terms of which are not as small as possible. We then prove that apparent singularities can be removed like in the univariate case by adding suitable additional solutions to the system at hand. The details can be found in [1].

References

[1] Y. Zhang, *Univariate contraction and multivariate desingularization of Ore ideals*, PhD thesis, Institute for Algebra, Johannes Kepler Univ., (2017).
http://www.algebra.uni-linz.ac.at/people/yzhang/yzhang_PhDthesis_final.pdf

Session 9

Geometry of Plane Curves

Session chairs:

Witold Mozgawa
Maria Curie-Skłodowska University (UMCS), Lublin, Poland

Waldemar Cieślak
Lublin University of Technology, Lublin, Poland

Thierry Dana-Picard
Jerusalem College of Technology, Jerusalem, Israel

Inflection points of bisoptic curves of conics

Th. Dana-Picard

Jerusalem College of Technology, ndp@jct.ac.il

Let be given a plane curve $\mathscr{C}$ and an angle θ. If it exists, the geometric locus of points through which passes a pair of tangents to $\mathscr{C}$ making an angle equal to θ is called an *isoptic curve* of $\mathscr{C}$. The name comes from the fact that from points on this geometric locus the curve $\mathscr{C}$ is seen under an angle equal to θ. If $\mathscr{C}$ is an ellipse and $\theta = 90^o$, the isoptic curve is the so-called director circle of the ellipse. The study of isoptic curves has been an active field of research for along time, both for strictly convex curves and for open curves; see for example [1], [7], [8].

With the developments of Computer Algebra Systems (CAS) and of Dynamical Geometry Systems (DGS), the study of isoptic curves has found new energies. In [2] and [3], it has been shown that if $\mathscr{C}$ is either an ellipse or a hyperbola, for a non-right angle, the isoptic curve is Spiric of Perseus (also called Oval of Cassini) (see [9], i.e. the intersection of a torus with a plane parallel to the axis of the torus; see Figure 1.

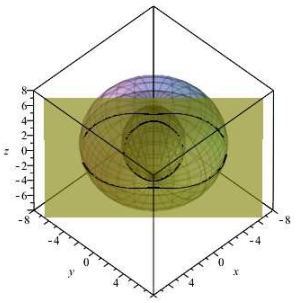


Figure 1: A spiric curve

Technology is used both to visualize the geometric situation and to solve the systems of equations yielded by the algebraic translation of the geometric data. For conic sections, the equations which have been obtained are non linear polynomial equations. The systems of equations have been solved using algorithms based on Gröbner bases computations; for this the polynomials are viewed as generating ideals in a polynomial ring. Partial results are obtained as a parametric representation of a curve, then implicitization is performed using similar techniques. A noticeable feature we have to deal with is that the curve may not be given by a single parametrization, but is rather presented as the union of numerous parameterized

arcs.

It must be mentioned that in order to obtain polynomial equations, squaring both sides is often used. The computations provide at the same time isoptic curves for angle θ and for $180^o - \theta$, whence the name *bisoptic* curves.

In this case, the bisoptic curve is the intersection of a self-intersecting torus with a plane parallel to the torus axis. The curve may be either a single closed curve or the union of two disjoint components. The curve may also have inflection points (flexes) or not, according to the distance from the plane to the torus axis.

In this paper, we study the existence of points of inflexion (flexes) for general spirics, using computations of Hessians. If the curve $\mathscr{C}$ is given by an implicit equation of the form $F(x,y) = 0$, then its Hessian curve is given by the vanishing points of the determinant $\det \frac{\partial d^2 F}{\partial x^i \, \partial y^j}$, for $i + j = 2$ (necessary condition, but not sufficient). The flexes of $\mathscr{C}$ are intersections of the curve with its Hessian curve ([4], [5]). The GeoGebra system is used for dynamical visualization, and the Maple software is used for automated study of the curves and their intersections. In particular, it must be noted that the equations involved here are of high degree (not less than 4).

References

[1] Cieślak. W., Miernowski, A and Mozgawa, W. : *Isoptics of a closed strictly convex curve*, in Global Differential Geometry and Global Analysis, Lecture Notes in Mathematics 1481, 28-35 (1991).

[2] Dana-Picard, Th., Mann, G. and Zehavi, N.: *From conic intersections to toric intersections: the case of the isoptic curves of an ellipse*, The Montana Mathematical Enthusiast 9 (1), 59-76. Available: http://www.math.umt.edu/TMME/vol9no1and2/index.html (2011).

[3] 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).

[4] Fulton, W.: Algebraic Curves: An Introduction to Algebraic Geometry, Amsterdam: W.A. Benjamin (1969).

[5] Kirwan, F.: Complex Algebraic Curves, London Mathematical Society Students Texts 23 (1992).

[7] Miernowski, A. and Mozgawa, W.: *On some geometric condition for convexity of isoptics*, Rendinconti Sem. Mat. Universita di Poi. Torino 55, 2 (1997).

[8] Szalkowski D.: *Isoptics of open rosettes*, Annales Universitatis Maria Curie - Sklodowska Lublin Polonia Vol. LIX Section A, 119-128 (2005).

[9] Wassenaar J.: Plane spiric curve, 2003. Available: http://www.2dcurves.com/quartic/quarticsp.html

On the closest distance between a point and a convex body

W. Cieślak[1], W. Mozgawa[2], P. Wlaź[1]

[1] *Lublin University of Technology, Department of Applied Mathematics, 20-618 Lublin, Nadbystrzycka 40, Poland,* izacieslak@wp.pl, p.wlaz@pollub.pl
[2] *Institute of Mathematics, Maria Curie-Skłodowska University, pl. M. Curie-Skłodowskiej 1, 20-031 Lublin, Poland,* mozgawa@poczta.umcs.lublin.pl

In this talk we fix a strictly convex body in the plane and a point in its exterior. We investigate the following problem with possible practical applications: find the point on the boundary of the fixed body, for which the distance to the given point is minimal. The focus of the paper is on the practical aspect of computational algorithm, which can be applied to obtain approximate or exact solution of the aforementioned problem.

Let C be a plane closed strictly convex curve, and the origin of coordinate system lies in the region bounded by C. We denote by p the support function of C with respect to the origin. The support function p is differentiable and the parametrization of C in terms of this function is given by

$$z(t) = p(t)e^{it} + \dot{p}(t)ie^{it}, \tag{1}$$

cf. [1]. We assume that $z(0)$ lies in the first quadrant. First we find the equation

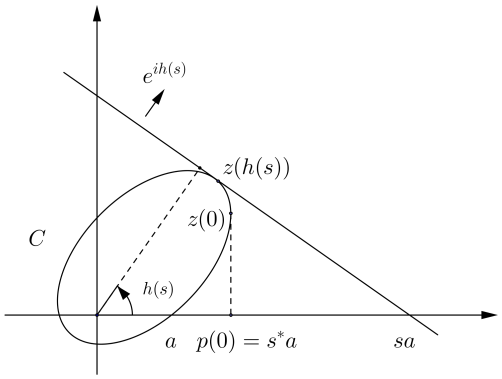


Figure 1: Definitions of a, $h(s)$, sa

of support line to C passing through a given point $(b,0)$, where $b > p(0)$. We introduce the notations as on the Figure 1, where h is a function of the variable

$s \in (s^*, +\infty)$ with values in the interval $\left(0, \frac{\pi}{2}\right)$. Let us introduce a function $f(u) = \frac{p(u)}{a\cos u}$. for $u \in \left(0, \frac{\pi}{2}\right)$. Then $f \circ h = \mathrm{id}$ and the function f is invertible, so if $b = sa$ then our support line has the following equation

$$x + y\tan f^{-1}\left(\frac{b}{a}\right) - b = 0. \tag{2}$$

In the further part of the talk we assume that C be a strictly convex curve given by (1) and $a = z(t^*) > 0$. If C satisfies the condition $\mathrm{Im}\, z(0) < 0$, then the function $Q\colon (0, t^*) \to \mathbf{R}$ given by the formula $Q(u) = -\frac{\dot{p}(u)}{a\sin u}$ is positive-valued and strictly decreasing. We then prove the main theorem of the talk

Theorem *Let C be a strictly convex curve given by* (1) *and $a = z(t^*) > 0$. If $b > a$ and* $\mathrm{Im}\, z(0) < 0$ *then the point $z\left(Q^{-1}\left(\frac{b}{a}\right)\right)$, realizes the shortest distance between $(b, 0)$ and C.*

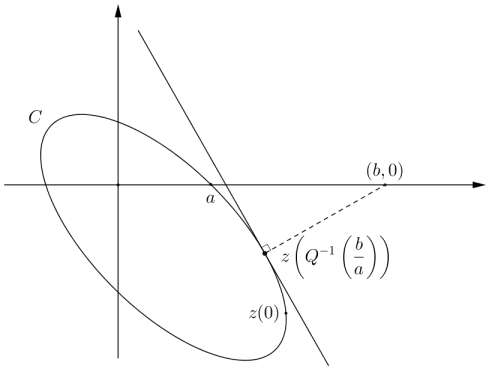


Figure 2: Point $z\left(Q^{-1}\left(\frac{b}{a}\right)\right)$ realizes the minimal distance

In general it is not trivial, or even impossible, to obtain the inverse of the function Q but at the end of the talk we describe how to approximate its inverse, which gives us the possibility of finding the approximation yielding the shortest distance between a given point and a strictly convex curve. We introduce an algorithm, which applies the ideas presented above which can be divided into two parts, the first one is to be done for a given convex set, the second one for a given point. The algorithm will be illustrated on two examples.

References

[1] Bonnesen, T.; Fenchel, W.; *Theorie der konvexen Körper*, Berlin-Heidelberg-New York: Springer-Verlag. (1974).

Isoptic curves of Fermat curves

Th. Dana-Picard[1], A. Naiman[2]

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

[2] *Jerusalem College of Technology, naiman@jct.ac.il*

Let be given a plane curve $\mathscr{C}$ and an angle θ. If it exists, the geometric locus of points through which passes a pair of tangents to $\mathscr{C}$ making an angle equal to θ is called an *isoptic curve* of $\mathscr{C}$. The name comes from the fact that from points on this geometric locus the curve $\mathscr{C}$ is seen under an angle equal to θ. The study of isoptic curves has been an active field of research for a long time, both for strictly convex curves and for open curves; see for example [2], [6], [7], [3] and [4].

We call Fermat curves the plane curves whose equation is of the form $x^k + y^k = 1$, where k is a non-negative integer. In [5], we considered paths of light trapped in Fermat curves, with a given number of reflection points. Theoretical developments, such as a general theorem by Birkhoff [1], saying that if the given curve is strictly convex, then such paths of light exist for any number of vertices, and in parallel, more elementary theorems from Calculus, ensured the existence of the paths of light under study, but their actual construction requested the solution of systems of two non linear equations. The usage of Gröbner bases packages led to contradictions: the output said that no solution. It appeared that the reason was that the reflection points have irrational coordinates, when the algorithms work over the rational numbers. Therefore work had to be performed using methods from numerical analysis and visualization has been obtained.

Denote by $\mathscr{C}$T one of these curves; it is a closed convex curve when the parameter k is even, and open otherwise (see Figure 1: the blue curve corresponds to $k = 4$, the green one to $k = 6$ and the red one to $k = 3$).

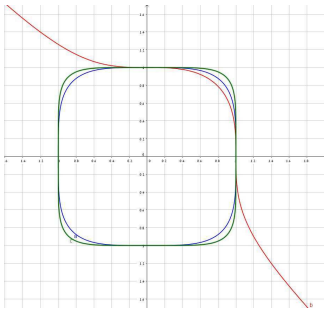


Figure 1: Different Fermat curves

For even k, the given curve defines a partition of the plane: through an interior point passes no tangent to $\mathscr{C}$, through a point on $\mathscr{C}$ there exists a unique tangent, and through an exterior point passes a pair of tangents (see Figure 2, which has been obtained during experimentations with the GeoGebra software).

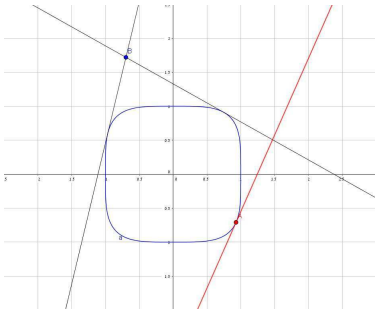


Figure 2: Tangents to a closed Fermat curve

Finding the tangents to $\mathscr{C}$ through a given exterior point requires the solution of a system of nonlinear equations. The situation here is similar to the above mentioned one, and a purely algebraic approach (i.e. via computations of Gröbner bases) does not yield a complete solution. Therefore, for various angles, we constructed isoptic curves of $\mathscr{C}$ using numerical methods.

In our talk we will present three approaches:

- a 2D, third order numerical approach which quickly yields a good visualization of the isoptic curves (see an example in Figure 3).
- a numerical approach of nonlinear fitting the (orthoganal or polar) mesh of θ values, to various families of functions, and
- an algebraic approach, using the **Gröbner** package of the software, with a discussion of the problems arising in the process.

These methods may be applied to generalized Fermat curves, we mean curves whose equation is of the form $|x|^k + |y|^k = 1$, where k may be any positive real number. When $k \geq 1$, the curve is strictly convex. If $k < 1$, the curve has cusps and the desired isoptic curve may be inside the given Fermat curve.

For our work, we use *Mathematica*, *Maple* and the Dynamical Geometry System *Geogebra*.

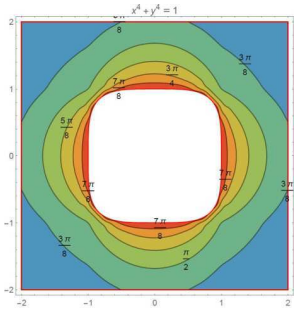


Figure 3: Numerical analysis of isoptics of a Fermat curve for $k = 4$

References

[1] Birkhoff, G.D. : *Dynamical Systems*, American Mathematical Society Colloquium Publications, Vol. IX, RI: Providence (1927).

[2] Cieślak, W., Miernowski, A and Mozgawa, W. : *Isoptics of a closed strictly convex curve*, in Global Differential Geometry and Global Analysis, Lecture Notes in Mathematics 1481, 28-35 (1991).

[3] Dana-Picard, Th., Mann, G. and Zehavi, N.: *From conic intersections to toric intersections: the case of the isoptic curves of an ellipse*, The Montana Mathematical Enthusiast 9 (1), 59-76. Available: http://www.math.umt.edu/TMME/vol9no1and2/index.html (2011).

[4] 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).

[5] Dana-Picard, Th. and Naiman, A. *Closed paths of light trapped in closed Fermat curves*, International Journal of Mathematical Education in Science and Technology 33 (6), 865-877 (2002).

[6] Miernowski, A. and Mozgawa, W.: *On some geometric condition for convexity of isoptics*, Rendinconti Sem. Mat. Universita di Poi. Torino 55, 2 (1997).

[7] Szałkowski D.: *Isoptics of open rosettes*, Ann. Univ. Mariae Curie-Skłodowska, Sect. A 59, 119-128 (2005).

Constructing Linkages for Drawing Plane Curves

M. Gallet[1], C. Koutschan[1], Z. Li[1], G. Regensburger[2], J. Schicho[2], N. Villamizar[1]

[1] *RICAM, Austrian Academy of Sciences, Austria, christoph.koutschan@ricam.oeaw.ac.at*
[2] *Johannes Kepler University Linz, Austria, josef.schicho@risc.jku.at*

We describe an application of computer algebra to the construction of mechanisms with certain prescribed properties. For this purpose, we have developed the package **PlanarLinkages** in Mathematica; it provides commands for constructing and visualizing planar linkages that draw a prescribed algebraic curve. The construction procedure is based on so-called motion polynomials; their basic arithmetic and a factorization algorithm is also provided by the package.

A *linkage* is a mechanical device consisting of rigid bodies (called *links*) that are connected by *joints*. We restrict our attention to *planar linkages*, i.e., to linkages all of whose links move in parallel planes. Moreover, we consider only *rotational joints*, i.e., we don't allow *prismatic joints*. We say that a linkage has *mobility one*, if it has only one degree of freedom; if we move a linkage of mobility one, the trace of any point located on one of the links yields a bounded curve in the plane.

The problem of constructing a planar linkage that draws a finite segment of a given algebraic curve was first addressed and solved in full generality by Kempe [2]. While his construction is very elegant in theory, it yields quite complicated linkages in practice. In a recent article [1], the symbolic computation group in Linz designed a novel algorithm for basically the same problem. The advantage of the new algorithm is that it yields much simpler linkages: the number of links and joints is only linear in the degree of the curve. Moreover, it allows for a simple collision detection, which for general linkages is a very hard problem. The drawback of our method is that it is only applicable to bounded rational curves, i.e., to curves that are parametrizable by rational functions and that are contained in some disk of finite radius.

A *motion* is a one-dimensional family of direct isometries (i.e., translations and rotations). We denote by SE_2 the special Euclidean group, which is the set of direct isometries in the plane with composition as the group operation. For a convenient treatment in a computer algebra system, we encode direct isometries as elements of the noncommutative $\mathbb{R}$-algebra $\mathbb{K}$ of *dual complex numbers*:

$$\mathbb{K} = \mathbb{C}[\eta] / (\eta^2, i\eta + \eta i).$$

Its elements are of the form $z + \eta w$ with complex numbers $z, w \in \mathbb{C}$, and according to the defining relations, which can be seen as rewriting rules, they are multiplied as follows:

$$(z_1 + \eta w_1) \cdot (z_2 + \eta w_2) = z_1 z_2 + \eta \, (\overline{z_1} w_2 + z_2 w_1). \tag{1}$$

By defining on $\mathbb{K}$ the equivalence relation

$$k_1 \sim k_2 \;:\Longleftrightarrow\; k_1 = \alpha k_2 \text{ for some } \alpha \in \mathbb{R} \setminus \{0\}, \tag{2}$$

we can show that the multiplicative group

$$\{z + \eta w \in \mathbb{K} \mid z \neq 0\} / \sim$$

is isomorphic to SE_2. A univariate polynomial in $\mathbb{K}[t]$ then gives rise to a one-dimensional family of direct isometries and is therefore called a *motion polynomial*. Motions that can be represented in this way are called *rational motions*. Our algorithm takes as input a motion polynomial and outputs a planar linkage of mobility one realizing the corresponding rational motion. This task is slightly more general than drawing a rational curve, since also the orientation of the end effector can be taken into account.

A motion polyomial $P = Z + \eta W \in \mathbb{K}[t]$ is called *bounded* if the complex polynomial $Z \in \mathbb{C}[t]$ does not have any real roots; the connection to the boundedness of the corresponding curve (the orbit of the origin) is established by the fact that Z appears as the denominator of its parametrization.

In order to construct a linkage that realizes the motion described by $P(t)$, we want to decompose it into simpler motions, namely into revolutions; these correspond exactly to motions that can be realized by a single (rotational) joint. We find [1, Lemma 4.3] that each linear motion polynomial, whose orbits are bounded, represents a revolute motion. Therefore, the desired decomposition is obtained by a factorization of P into linear polynomials; we present an algorithm for this task.

The factorization allows us to construct a linkage, in the form of an open chain, whose links can move according to the revolutions represented by the linear factors. Since such a linkage has many degrees of freedom, we need to constrain its mobility. This is done by adding more links and joints, which is achieved by an iteration of the so-called flip procedure [1, Sections 6–7].

References

[1] M. Gallet, C. Koutschan, Z. Li, G. Regensburger, J. Schicho, and N. Villamizar. *Planar linkages following a prescribed motion*, Mathematics of Computation **86**, pp. 473–506, 2017. To appear (preprint on arXiv:1502.05623), DOI: 10.1090/mcom/3120.

[2] A. B. Kempe. *On a general method of describing plane curves of the n^{th} degree by linkwork*, Proceedings of the London Mathematical Society, s1-7(1), pp. 213–216, 1876.

[3] C. Koutschan. *Mathematica package PlanarLinkages and electronic supplementary material for the paper "Planar linkages following a prescribed motion"*, 2015. Available at `http://www.koutschan.de/data/link/`.

Session 10

Automated Theorem Proving in Dynamic Geometry

Session chairs:

Zoltán Kovács
The Private University College of Education of the Diocese of Linz, Austria

Pavel Pech
University of South Bohemia, Ceske Budejovice, Czech Republic

Tomás Recio
University of Cantabria, Spain

Computer-mediated thinking

R. M. Corless

ORCCA and the Department of Applied Mathematics, University of Western Ontario, Canada, rcorless@uwo.ca

This talk discusses computer-mediated thinking and some of its possible implications for curriculum design in mathematics education. We begin with a discussion of today's context and of ideas related to computer-mediated thinking. We continue with examples of the use of computer-mediated thinking in modern applied mathematics. We then extract some suggestions for a curriculum in mathematics centred at the calculus level. We include specific suggestions for removing material from the current syllabus. We end with a discussion of the unintentional power of the calculus.

Automated study of a curve and its associated curves: the case of an astroid

Th. Dana-Picard

Jerusalem College of Technology, ndp@jct.ac.il

In [1] and [2] we studied isoptic curves of conics and showed a unifying framework for conics (in 2D) and toric sections (in 3D). In other works such as [3], we studied envelopes of parametric families of plane curves, etc. A common aspect of these works relies in the double trend, geometrical experiments using technology and algebraic proofs relying on the solution of non linear polynomial equations. For this, we used packages relying on the computation of Gröbner bases.

In this talk, we focus on one family of curves, namely astroids, and study various aspects of it using CAS or DGS. Denote by $\mathscr{C}$ by the following equivalent definitions:

- An *implicit* equation: $|x|^{\frac{2}{3}} + |y|^{\frac{2}{3}} = k$, $k > 0$;
- A *parametric* presentation $(x(t), y(t)) = \left(a\ \cos^3 t, a\ \sin^3 t\right)$, $t \in [0, 2\pi]$, where a is a non negative real number.

WLOG we work with $k = a = 1$. The curve is displayed in Figure 1.

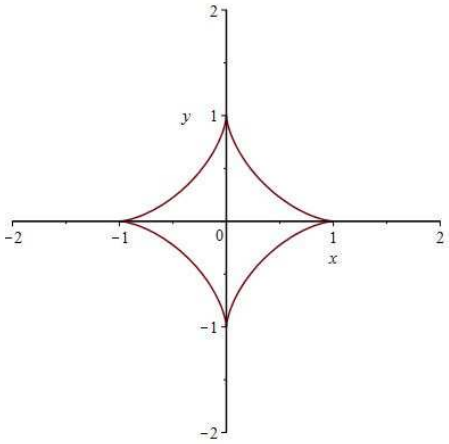


Figure 1: An astroid

From another point of view, this curve can be obtained as the envelope of the family of segments with fixed length (in our case the length is equal to 1) and

whose endpoints are on the coordinate axes. Translating the data into polynomial equations is a central issue.

Using technology, we study the astroid (C) as an envelope. Afterwards we study the *orthoptic curve* of the astroid $\mathscr{C}$, namely the geometric locus of the points through which pass two perpendicular tangents to the astroid; see Figure 2. This is a well-known question when dealing with conics, but much less with other curves. The curve which is found is a 4-folium, which can be viewed also as the projection onto the plane of a specific space curve. We have here a new case where a unified study, both in 2D and in 3D, of geometrical objects can be performed.

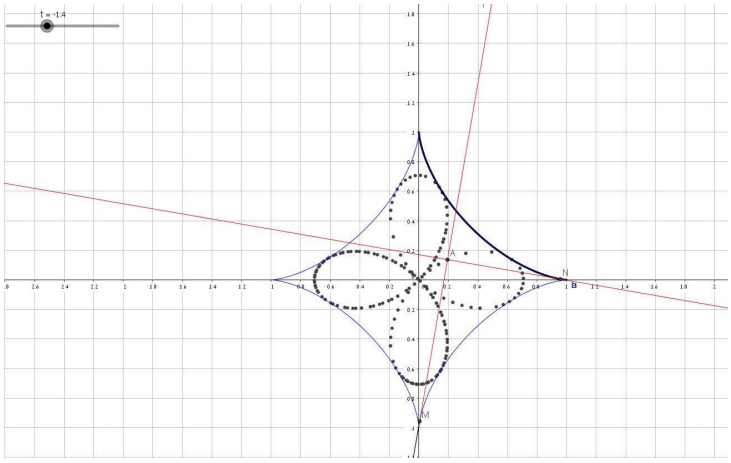


Figure 2: The orthoptic of the astroid

The orthoptic curve is non convex and has a singular point. We refer to [4] for conditions for convexity of an isoptic curve.

In this talk, we will discuss various methods, and also how to generalize the question to any angle, i.e. how we can study other isoptic curves of $\mathscr{C}$. The experimental part of the work is performed using Maple and GeoGebra. Of course, for building curves, the slider bar available in GeoGebra (or, as an alternative, the "Move" feature), is a central tool.

References

[1] Th. Dana-Picard, G. Mann and N. Zehavi, *From conic intersections to toric intersections: the case of the isoptic curves of an ellipse*, The Montana Mathematical Enthusiast 9 (1), 59-76. Available: `http://www.math.umt.edu/TMME/vol9no1and2/index.html` (2011).

[2] Th. Dana-Picard, G. Mann and N. Zehavi, *Bisoptic curves of a hyperbola*, International Journal of Mathematical Education in Science and Technology **45 (5)**, pp. 762-781 (2014).

[3] Th. Dana-Picard and N. Zehavi, *Automated Study of Envelopes: transition from 1-parameter to 2-parameter families of surfaces*, to appear in Proceedings of CADGME 2016 (Z. Lavicza and C. Sarvari, eds.), The Electronic Journal of Mathematics and Technology (2017).

[4] A. Miernowski and W. Mozgawa, *On some geometric condition for convexity of isoptics*, Rendinconti Sem. Mat. Universita di Poi. Torino 55, 2 (1997).

Automated theorem proving in school mathematics

R. Hašek

University of South Bohemia, Czech Republic, hasek@pf.jcu.cz

Particular examples of possible ways to utilize the methods and tools of automated theorem proving in secondary school mathematics teaching and learning will be presented. Questions on the current use of these methods and their perspectives in school mathematics will also be issued.

References

[1] F. Botana, M. Hohenwarter, P. Janičič, Z. Kovács, I. Petrovič, T. Recio and S. Weitzhofer, *Automated Theorem Proving in GeoGebra: Current Achievements*, Journal of Automated Reasoning, **55**(1), pp. 39-59 (2015).

[2] H. S. M. Coxeter and S. L. Greitzer, *Geometry revisited* (2. printing). Washington: Math. Assoc. of America (1967).

[3] S. C. Chou, X. S. Gao and C. C. Chang, *Machine proofs in geometry: automated production of readable proofs for geometry theorems* (1st ed.). New Jersey: World Scientific (1994).

[4] H. R. Jacobs, *Geometry: seeing, doing, understanding* (3rd ed.). New York: W.H. Freeman and Co. (2003).

[5] Z. Kovács, *Computer Based Conjectures and Proofs in Teaching Euclidean Geometry* (dissertation). Linz (2015).

[6] P. Pech, *Selected topics in geometry with classical vs. computer proving* (1st ed.). Singapore: World Scientific (2007).

[7] P. Quaresma, Towards an Intelligent and Dynamic Geometry Book. *Mathematics In Computer Science* (2017).

[8] P. Quaresma and V. Santos, Visual Geometry Proofs in a Learning Context [Online]. In *ThEdu'15: The 4th International Workshop on Theorem proving components for Educational software. 8th Conference on Intelligent Computer Mathematics CICM 2015 July 13-17, 2015 Washington DC, USA*, Universidade de Coimbra, pp. 1-8 (2015).

Achievements and challenges in automatic locus and envelope animations in dynamic geometry environments

Z. Kovács

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

Recent researches on computing Gröbner bases significantly faster than earlier opened the road to manipulate on tens of equation systems in many variables within a second. Thus nowadays it is possible to create real-time interactive animations based on purely symbolic computations. Such real-time dynamic geometry animations include computing and plotting locus or envelope equations for geometry constructions on various software platforms [1].

We highlight GeoGebra's [2] animation related features on using such heavy computations. By analyzing more than 100 of test cases we can classify locus/envelope problems into *smooth*, *lagging*, *heavy* and *infeasible* sets. Our database at `http://dev.geogebra.org/trac/browser/trunk/geogebra/test/scripts/benchmark/art-plotter` is continuously tested against GeoGebra's current source code on a daily basis and evaluated at `https://prover-test.geogebra.org/job/GeoGebra-art-plottertest/ws/test/scripts/benchmark/art-plotter/html/all.html` by using the Jenkins open source automation server for multiple platforms.

The classification allows us to propose some novel methods [3] in computer aided teaching of planar geometry in the classrooms. On the other hand, we call for collaboration to attempt handling non-smooth problems by working together with authors of open source implementations of efficient elimination algorithms.

This on-going work is a cooperation with F. Botana, B. Parisse, T. Recio and M. P. Vélez.

References

[1] Z. Kovács, *Real-time Animated Dynamic Geometry in the Classrooms by Using Fast Gröbner Basis Computations*. Mathematics in Computer Science **11(1)**, doi:10.1007/s11786-017-0308-2 (2017).

[2] M. Hohenwarter, *Ein Softwaresystem für dynamische Geometrie und Algebra der Ebene.* Master's thesis. Salzburg: Paris Lodron University (2002).

[3] M. A. Abánades, F. Botana, Z. Kovács, T. Recio and C. Sólyom-Gecse, *Development of automatic reasoning tools in GeoGebra*. ACM Communications in Computer Algebra **50(3)** pp. 85-88, November (2016).

Investigation of geometric loci using DGS and CAS

J. Blažek[1], P. Pech[2]

[1] *University of South Bohemia, Czech Republic, blazej02@pf.jcu.cz*
[2] *University of South Bohemia, Czech Republic, pech@pf.jcu.cz*

The tool *Locus* belongs to one of traditional functions of dynamic geometry systems (DGS). We cannot use it always, to its application we need two points. The first point is a mover, the point which usually moves along a certain object. The second point—a tracer—is somehow dependent on the mover and draws the sought trajectory. The command *Locus* is very simple and useful, its disadvantage is that we cannot apply it to every problem. Problems that we will present in the talk are of this case.

To determine these problems we have to use a more advanced tool *LocusEquation* which has recently been implemented into GeoGebra version 5 (see [1] and [3]). This command brings a completely new approach in searching for loci. This approach belongs to automated discovery [8], the part of the theory of automated theorem proving [5]. The tool is based on elimination of variables in a system of algebraic equations describing the locus. It returns an implicit equation of a curve. It is well known that the result is the Zarisky closure of a projection on the space of local coordinates [6]. This often leads to the fact that instead of a real locus we get the smallest variety which contains, besides the locus, also some extraneous objects not pertaining to it. Before using the command *LocusEquation* we have to construct in GeoGebra a geometric diagram describing the locus. After constructing the diagram we apply the command *LocusEquation* which has two parameters. The first one is the thesis T (which must be a Boolean expression), the second one is a free point P whose locus we investigate. The result of *LocusEquation* [T,P] produces the set V such that "if T is true then $P \in V$" (see [2]).

Several Boolean expressions in the form of commands such as *AreCollinear* or *AreConcyclic* are tested in some examples which results to various loci, usually curves, in the plane (see [7]). Here we encounter problems which can occur in loci investigation and which could be possibly solved in the future.

By searching for the locus we will apply Groebner bases and Wu–Ritt characteristic methods using software CoCoA [4] and Epsilon library [9].

References

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

[2] M. A. Abánades, F. Botana, Z. Kovács, T. Recio and C. Sólyom-Gecse, *Implementing automatic discovery in GeoGebra*, Proceedings of ADG 2016, Strasbourg (2016).

[3] F. Botana, M. Hohenwarter, P. Janičič, Z. Kovács, I. Petrovič, T. Recio and S. Weitzhofer, *Automated Theorem Proving in GeoGebra: Current Achievements*, Journal of Automated Reasoning *55*, pp. 39-59 (2015).

[4] A. Capani, G. Niesi and L. Robbiano, *CoCoA, a System for Doing Computations in Commutative Algebra*, `http://cocoa.dima.unige.it`

[5] S. C. Chou, *Mechanical Geometry Theorem Proving*, D. Reidel Publishing Company, Dordrecht (1987).

[6] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties and Algorithms*, Springer, Berlin (1997).

[7] E. V. Shikin, *Handbook and Atlas of Curves*, CRC Press, Boca Raton (1995).

[8] T. Recio and M. P. Vélez, *Automatic discovery of theorems in elementary geometry*, Journal of Automated Reasoning **23**, pp. 63-82 (1999).

[9] D. Wang, *Epsilon: A library of software tools for polynomial elimination*, in *Mathematical Software*, (A. Cohen, X. S. Gao and N. Takayama, eds). World Scientific, Singapore New Jersey, pp. 379-389 (2002). `http://www-calfor.lip6.fr/~wang/epsilon/`

Automated Reasoning Tools in GeoGebra

T. Recio

University of Cantabria, Spain, tomas.recio@unican.es

GeoGebra [4] is a dynamic geometry software with tenths of millions users worldwide. Despite its original merely graphical flavor, successful attempts were performed during the last years towards combining standard dynamic geometry approaches with automated reasoning methods using computer algebra tools.

Since Automated Theorem Proving (ATP) in geometry has reached a rather mature stage, a multinational group (see the authors of [2] for a partial relation of its members) started in 2010 a project of incorporating and testing a number of different automated geometry provers in GeoGebra. This collaboration was built upon previous approaches and achievements of a large community of researches, involving different techniques from algebraic geometry and computer algebra. Moreover, various symbolic computation, open source, packages have been involved, most importantly the Singular [3] and the Giac [8] computer algebra systems. See [6] and [7] for a more detailed overview.

As a result of this collaboration, we have been able to recently announce the implementation [1] of three automated reasoning tools (ART) in GeoGebra, all of them working in the desktop, web, tablet or smartphone versions of GeoGebra: the automated derivation of (numerical) properties in a given construction, by means of the *Relation Tool*; the verification of the symbolic truth of these properties, by means of the *Prove* and *ProveDetails* tools; and the discovery of missing hypotheses for a conjectural statement to hold true, through the *LocusEquation* tool.

The *Relation Tool*, in its original form, allows selecting two geometrical objects in a construction, and then to check for typical relations among them, including perpendicularity, parallelism, equality or incidence. Finally, it shows a message box with the obtained information (yes/no the relation holds). GeoGebra version 5 now displays an extra button in the message box with the caption "More..." which results in some symbolic computations when pressed. That is, by pressing the "More..." button, GeoGebra's Automatic Theorem Proving subsystem starts and selects (by some heuristics) an appropriate prover method to decide if the numerically obtained property is indeed absolutely true in general. The current version of GeoGebra is capable of choosing a) the Gröbner basis method, b) Wu's characteristic method, c) the area method, or d) sufficient number of exact checks, deterministic method (see [5] and [9]), as the underlying ATP technique addressed by the *Prove* command. See [7] for more details on this portfolio prover.

Moreover, if the conjectured relation does not (mathematically speaking) hold,

the first two methods can determine some geometrical extra-conditions, which need to hold true in order to make the given statement generally correct, either using the *ProveDetails tool* (in the generally true case) or the *LocusEquation* tool (in the generally false case).

In the talk I will outline, through examples, some features of the ART in GeoGebra, providing some details on the underlying algebraic methods and reporting on our current work-in-progress concerning this topic, done in cooperation with F. Botana, Z. Kovács and M.P. Vélez.

Acknowledgement: Partially supported by the Spanish Ministerio de Economía y Competitividad and by the European Regional Development Fund (ERDF), under the Project MTM2014-54141-P.

References

[1] M.A. Abánades, F. Botana, Z. Kovács, T. Recio and C. Sólyom-Gecse, *Development of automatic reasoning tools in GeoGebra*. ACM Communications in Computer Algebra **50(3)** pp. 85-88, November (2016).

[2] F. Botana, M. Hohenwarter, P. Janičić, Z. Kovács, I. Petrović, T. Recio and S. Weitzhofer, *Automated theorem proving in GeoGebra: current achievements*. Journal of Automated Reasoning, **Vol. 5, No. 1**, pp-39-59, (2015).

[3] W. Decker, G-M. Greuel, G. Pfister, H. Schönemann, *Singular 3-1-6 , A computer algebra system for polynomial computations*. `http://www.singular.uni-kl.de`. (2012).

[4] M. Hohenwarter, *Ein Softwaresystem für dynamische Geometrie und Algebra der Ebene.* Master's thesis. Salzburg: Paris Lodron University. (2002).

[5] Z. Kovács, T. Recio and S. Weitzhofer, *Implementing theorem proving in GeoGebra by exact check of a statement in a bounded number of test cases.* In: *Proceedings EACA 2012, Libro de Resúmenes del XIII Encuentro de Álgebra Computacional y Aplicaciones*. Universidad de Alcalá, pp. 123–126. (2012).

[6] Z. Kovács, *Computer based conjectures and proofs.* Doctoral Dissertation. Linz: Johannes Kepler University. (2015).

[7] Z. Kovács, *The Relation Tool in GeoGebra 5*. In Botana, F., Quaresma, P. (Eds.), *Post-conference Proceedings of the 10th International Workshop on Automated Deduction in Geometry (ADG 2014),* 9-11 July 2014, Lecture Notes in Artificial Intelligence **9201**, pp. 53-71. Springer. (2015).

[8] B. Parisse, *Giac/Xcas, a free computer algebra system*, Available at `http://www-fourier.ujf-grenoble.fr/~parisse/giac.html`. (2013).

[9] S. Weitzhofer, *Mechanic proving of theorems in plane geometry.* Master's thesis, Johannes Kepler University, Linz, Austria. `http://test.geogebra.org/~kovzol/guests/SimonWeitzhofer/DiplArbeit.pdf`. (2013).

Session 11

Algebraic Methods in Geometric Modeling

Session chairs:

Gershon Elber
Computer Science, Department Technion, Haifa, Israel

Myung Soo Kim
Computer Science Department, Seoul national University, Seoul Korea

On the computation of the straight lines contained in a rational surface.

J.G. Alcázar[1], J. Caravantes[2]

[1] *Universidad de Alcalá, Madrid, Spain, juange.alcazar@uah.es*
[2] *Universidad Complutense, Madrid, Spain, jcaravan@mat.ucm.es*

Straight lines are certainly notable curves in an algebraic surface. Probably the most famous result on algebraic surfaces containing straight lines is related to cubic surfaces: G. Salmon [3], after correspondence with A. Cayley, proved that projective smooth cubic surfaces contain exactly 27 (projective, complex and real) straight lines, some of them at infinity. These surfaces happen to be rational, and one can compute the straight lines contained in the surface from the base points of the parametrization [2].

However, unlike cubics, surfaces of degree higher than 3 do not necessarily contain straight lines. Furthermore, in the affirmative case, up to our knowledge there is no known algorithm other than the brute-force approach to find them. In this talk we will present the ideas in [1] to solve the problem of determining the straight lines contained in a surface defined by a rational parametrization of any degree. The main idea is to exploit the well-known result in Differential Geometry that characterizes real non-singular straight lines contained in a surface, as curves that are simultaneously asymptotic lines, and geodesics. This characterization provides *differential* conditions to find the straight lines contained in the surface, that we transform into *algebraic conditions*; this way, we can take advantage of classical methods in polynomial algebra, mainly factoring and resultants, to solve the problem. Other special straight lines, in particular the ones contained in the singular part of the parametrization, can also be found. Additionally, the same method allows to compute the complex straight lines contained in the surface too.

References

[1] J.G. Alcázar, J. Caravantes *On the computation of the straight lines contained in a rational surface*, ArXiv 1603.03959, (2016).

[2] C.L. Bajaj, R.J. Holt, A.R. Netravali *Rational parametrization of non-singular real cubic surfaces*. ACM Transactions on Graphics 17, 1-31, (1998).

[3] G. Salmon *A Treatise on the Analytic Geometry of Three Dimensions, vol. I and II.* Chelsea Publishing, (1914).

Modeling and rationalization of free-form surfaces

M. Bartoň[1]

[1] *Basque Center for Applied Mathematics (BCAM), Bilbao, Spain, mbarton@bcamath.org*

Free-form surfaces are a popular modeling tool for engineers, architects, and designers in general. Most commonly represented as non-uniform rational B-splines (NURBS), these surfaces are supported by a vast majority of the state-of-the-art computer-aided design (CAD) software. Using such software, the modeling stage of a free-form surface is intuitive via local adjustment of the control points. In contrast, the manufacturing (or rationalization) stage is difficult, particularly because of the very diverse nature of a general free-form surface.

In this talk, I will discuss our recent work in this reverse engineering direction and discuss possibilities and limitations of geometrical approaches that aim at approximating general free-form geometry by manufacturable patches. In particular, I will briefly discuss three projects that use circular arc splines [1], sweeps of planar profiles [2], and envelopes of surfaces of revolution [3]. Finally, I will indicate future research directions that point towards manufacturing-aware modeling, i.e., a methodology that directly considers the manufacturing technology already in the modeling stage.

References

[1] Bartoň M., Shi L., Killian M., Wallner J., Pottmann H. Circular arc snakes and kinematic surface generation, *Computer Graphics Forum*, 32 (1), 1-10, 2013.

[2] Bartoň M., Pottmann H., Wallner J. Detection and reconstruction of freeform sweeps, *Computer Graphics Forum*, 33 (2), 23-32, 2014.

[3] Bo P., Bartoň M., Plakhotnik D., Pottmann H. Towards efficient 5-axis flank CNC machining of free-form surfaces via fitting envelopes of surfaces of revolution, *Computer Aided Design* 79, 1–11, 2016.

Precise Construction of Micro-structures and Porous Geometry via Functional Composition

G. Elber[1]

[1] *Technion, Israel, gershon@cs.technion.ac.il*

We introduce a modeling constructor for micro-structures and porous geometry via curve-trivariate, surface-trivariate and trivariate-trivariate function (symbolic) compositions. By using 1-, 2- and 3-manifold based tiles and paving them multiple times inside the domain of a 3-manifold deforming trivariate function, smooth, precise and watertight, yet general, porous/micro-structure geometry might be constructed, via composition. The tiles are demonstrated to be either polygonal meshes, (a set of) Bézier or B-spline curves, (a set of) Bézier or B-spline (trimmed) surfaces, (a set of) Bézier or B-spline (trimmed) trivariates or any combination thereof, whereas the 3-manifold deforming function is either a Bézier or a B-spline trivariate.

We briefly lay down the theoretical foundations, only to demonstrate the power of this modeling constructor in practice, and also present a few 3D printed tangible examples. We will then discuss these results and conclude with some future directions and limitations.

References

[1] G. Elber. *Precise Construction of Micro-structures and Porous Geometry via Functional Composition.* To apear in the Proceedings of the 9th International Conference on Mathematical Methods for Curves and Surfaces (MMCS9), Tonsberg, Norway, June 2016.

Solving Multivariate Polynomial Systems using Hyperplane Arithmetic and Linear Programming

I. Hanniel[1]

[1] *Technion, currently at Mobileye Vision Technologies Ltd., iddo.hanniel@mobileye.com*

Solving polynomial systems of equations is an important problem in many fields such as computer-aided design and manufacturing [1] and robotics [2]. In recent years, subdivision-based solvers, which typically make use of the properties of the Bézier / B-spline representation, have proven successful in solving such systems of polynomial constraints [3, 4, 5]. A major drawback in using subdivision solvers is their lack of scalability [6]. When the given constraint is represented as a tensor product of its variables, it grows exponentially in size as a function of the number of variables.

In this paper, we present a new method for solving systems of polynomial constraints, which scales nicely for systems with a large number of variables and relatively low degree. Such systems appear in many application domains. The method is based on the concept of *bounding hyperplane arithmetic*, which can be viewed as a generalization of interval arithmetic [7]. We construct bounding hyperplanes, which are then passed to a linear programming solver in order to reduce the root domain. We have implemented our method and present experimental results. The method is compared to previous methods and its advantages are discussed.

References

[1] N. Patrikalakis and T. Maekawa. *Shape Interrogation for Computer Aided Design and Manufacturing*. Mathematics and Visualization. Springer, 2002.

[2] J.-P. Merlet. *Parallel Robots*. Solid mechanics and its applications. Kluwer, 2005.

[3] G. Elber and M.-S. Kim. Geometric constraint solver using multivariate rational spline functions. In *SMA 2001: Proceedings of the Sixth ACM Symposium on Solid Modeling and Applications*, pages 1–10. ACM, 2001.

[4] E. C. Sherbrooke and N. M. Patrikalakis. Computation of the solutions of nonlinear polynomial systems. *Computer Aided Geometric Design*, 10(5):379–405, 1993.

[5] B. Mourrain and J. P. Pavone. Subdivision methods for solving polynomial equations. *J. Symb. Comput.*, 44(3):292–306, Mar. 2009.

[6] G. Elber and T. A. Grandine. An efficient solution to systems of multivariate polynomial using expression trees. *IEEE Trans. Vis. Comput. Graph.*, 15(4):596–604, 2009.

[7] R. E. Moore, R. B. Kearfott, and M. J. Cloud. *Introduction to Interval Analysis*. SIAM, 2009.

Efficient Algorithms using Dynamic Bounding Volume Hierarchy for Freeform Geometric Shapes under Deformation

M.-S. Kim[1]

[1] *Seoul National University, South Korea, mskim@snu.ac.kr*

We consider the construction of dynamic bounding volume hierarchy (BVH) for planar freeform curves and surfaces under deformation. The dynamic BVH construction is compared with conventional spatial data structures. The effectiveness of our BVH structure is then demonstrated using a few test examples of designing efficient algorithms for freeform geometric shapes under deformation.

In collaboration with Gershon Elber, Yong-Joon Kim, and Jaewook Lee

Efficient methods for roots of univariate scalar Bèziers

Jinesh Machchhar[1], Gershon Elber[1]

[1] *Technion-Israel Institute of Technology, Israel, {jineshmac, gershon}@cs.technion.ac.il*

Finding roots of polynomials is a fundamental problem lying at the core of many applications in science and engineering. For instance, defining manifolds implicitly, computing intersection of manifolds, computing offsets and sweeps, kinematic analysis/synthesis, etc. In this work we focus on finding zeros of univariate scalar polynomials. We choose the Bernstein basis for the representation due to their several desirable properties such as numerical stability, convex-hull property and variation diminishing property.

Traditional methods for numerically computing the zeros of univariate scalar Bèziers [2] employ subdivision to recursively subdivide the interval of interest, in the middle, until either the topology of the interval is known or the width of interval falls below the specified subdivision tolerance. Once the topology of the interval is known, a numerical method such as Newton-Raphson is employed to locate the roots within specified numerical tolerance.

In contrast, our method [5] begins by guessing one of the roots using the Newton-Raphson method. The Bèzier polynomial is then subdivided at the root. The two resulting polynomials have roots at their respective end-points which are factored out algebraically in order to obtain polynomials of lower degree. The algorithm then recurses on these polynomials. The reduction in the degree of polynomials results in reduces complexity of the problem and higher computational efficiency.

A salient feature of our algorithm is the ability to count the multiplicities of roots. This is done by inspecting the terminal coefficient of the polynomial obtained after factoring out root at the respective end-point of the domain. If this coefficient is found to be zero, within specified numerical tolerance, then it indicates the presence of a repeated root, which is again factored out.

The algorithm is implemented in the IRIT [1] solid modeling kernel. Comparison of running times of our method with previous state of the art [3, 4] over polynomials of varying degrees shows about an order-of-magnitude speed-up.

References

[1] Gershon Elber, *IRIT modeling environment*, `http://www.cs.technion.ac.il/~irit/`.

[2] Jeffrey M. Lane and Richard F. Riesenfeld, *Bounds on a polynomial*, in *BIT Numerical Mathematics*, 21(1), pp. 112-117 (1981).

[3] Thomas W. Sederberg and Scott R. Parry, *Comparison of three curve intersection algorithms*, in Computer-Aided Design, 18(1), pp. 58-63 (1986).

[4] Thomas W. Sederberg and Ray J. Meyers, *Loop detection in surface patch intersections*, in Computer Aided Geometric Design, 5(2), pp. 161-171 (1988).

[5] Jinesh Machchhar and Gershon Elber, *Revisiting the Problem of Zeros of Univariate Scalar Béziers*, in Computer Aided Geometric Design, 43(c), pp. 16-26 (2016).

Rational parametrizations of Darboux and isotropic cyclides

R. Krasauskas[1], S. Zube[1]

[1] *Vilnius University, Vilnius, Lithuania, severinas.zube@mif.vu.lt*

Darboux [2] and isotropic [4] cyclides are projections of intersections of certain pairs of quadrics in P^4. Therefore, they are particular cases of real Del Pezzo surfaces, that are are known to be rational. Cyclides are important for modeling applications because they contain several families of circles (Darboux case), and because they are dual to certain surfaces with rational offsets (isotropic case). There are three topological types of real cyclides: torus topology T^2, one real spherical component S^2, or two real spherical components $S^2 \sqcup S^2$. The latter case is the most complicated, since $\mathbb{R}$-birational parametrization is not possible, and one can only hope to parametrize both components separately.

In this talk we represent rational parametrizations of cyclides described in Clifford–Bézier formulas. Let $\mathscr{A}P^1$ be a projective line over two cases of Clifford algebras $\mathscr{A} = Cl(\mathbb{R}^3), Cl(\mathbb{R}^{2,0,1})$, generated by euclidean space $\mathbb{R}^3$ and pseudo-euclidean space $\mathbb{R}^{2,0,1}$ with signature $(++0)$. Our approach is to treat $\mathscr{A}P^1$ as an ambient space and to consider toric Bezier patches in the corresponding homogeneous coordinates. It is proved that such patches of formal degree 2 with standard and non-standard real structures cover all cases of real Darboux and isotropic cyclides. In particular, the case with T^2 topology has parametrization of bidegree $(1,1)$, and one component of case $S^2 \sqcup S^2$ can be parametrized with bidegree $(2,1)$ in the corresponding Clifford algebra terms.

The MAPLE package "Clifford" [1] was essential for all our results that were derived using symbolic computations. We employ the Clifford algebra $Cl(\mathbb{R}^3)$ for Darboux cyclides. It is remarkable that the same formulas generate parametrizations of isotropic cyclides if one uses the Clifford algebra $Cl(\mathbb{R}^{2,0,1})$ instead.

Recently, studying low degree rational patches on isotropic cyclides in [4], we noticed relations with offsets of quadrics. Oriented tangent planes of a given quadric in $\mathbb{R}^3$ define a surface on the Blaschke cylinder, which is actually an isotropic cyclide, i.e. dual to quadric. In the standard way [3], using duality, we obtain the offset stable parametrization of the quadric. In particular, the following offset bidegrees are obtained: $(4,4)$ for one-sheeted hyperboloids and hyperbolic paraboloids, $(4,8)$ for ellipsoids and two-sheeted hyperboloids. It seems the obtained degrees are minimal.

References

[1] R. Ablamowich *A Maple 13 Package for Clifford Algebra Computations Version 13.3*, http://math.tntech.edu/rafal/cliff13/index.html, 2012

[2] H. Pottmann, L. Shi, M. Skopenkov, *Darboux cyclides and webs from circles* , Comput. Aided Geom. Des., **29**, pp. 77–97 (2012).

[3] R. Krasauskas, M. Peternell, *Rational offset surfaces and their modeling applications*. In: IMA **151**: Nonlinear Computational Geometry, I.Z. Emiris, F. Sottile, and Th. Theobald (eds.), pp. 109–135, (2010).

[4] R. Krasauskas, S. Zube, S. Cacciola, *Bilinear Clifford-Bezier Patches on Isotropic Cyclides*. In: Mathematical Methods for Curves and Surfaces, Lect. Notes Comput. Sc., **8177**, 283–303, (2014).

Session 12

Katsusuke Nabeshima, Tokushima University, Japan

Session chairs:

Yosuke Sato
Tokyo University of Science, Japan

On Multivariate Hermitian Quadratic Forms

R. Fukasaku[1], H. Iwane[2]

[1] *Tokyo University of Science, Tokyo, Japan, fukasaku@rs.tus.ac.jp*
[2] *Fujitsu Laboratories LTD/National Institute of Informatics, Kanagawa/Tokyo, Japan, iwane@jp.fujitsu.com*

Quantifier elimination over real closed fields (real QE) is an important area of research for various fields of mathematics and computer science. Though the cylindrical algebraic decomposition (CAD) algorithm introduced by G. E. Collins [4] and improved by many successive works has been considered as the most efficient method for a general real QE problem up to the present date, we may have a more practical method for a special type of real QE problems.

When the given quantified formula contains many equalities, before directly applying the CAD algorithm we can eliminate all possible quantifiers using the underlying equational constraints by the method introduced in [9]. The essential part of the method is the algorithm which eliminates all quantifiers $\exists \bar{X} (= \exists \bar{X}_1 \cdots \exists \bar{X}_n)$ from the following basic first order formula based on the theory of real roots counting by multivariate Hermitian quadratic forms introduced in [1, 7]:

$$\phi(\bar{A}) \wedge \exists \bar{X} \ (f_1(\bar{A},\bar{X}) = 0 \wedge \cdots \wedge f_s(\bar{A},\bar{X}) = 0 \wedge h_1(\bar{A},\bar{X}) > 0 \wedge \cdots \wedge h_t(\bar{A},\bar{X}) > 0),$$

where $f_1,\ldots,f_s,h_1,\ldots,h_t$ are polynomials in $\mathbf{Q}[\bar{A},\bar{X}] (= \mathbf{Q}[A_1,\ldots,A_m,X_1,\ldots,X_n])$ such that the parametric ideal $I = \langle f_1,\ldots,f_s \rangle$ is zero-dimensional for any specialization of the variables $\bar{A}$ satisfying $\phi(\bar{A})$. The algorithm computes a comprehensive Gröbner system (CGS) of I regarding $\bar{A}$ as parameters, then computes the multivariate Hermitian quadratic form $M^I_{h_1^{e_1}\cdots h_t^{e_t}}$ for each $(e_1,\ldots,e_t) \in \{1,2\}^t$ and produces the following equivalent quantifier free formula:

$$\sum_{(e_1,\ldots,e_t)\in\{1,2\}^t} \mathrm{sign}(M^I_{h_1^{e_1}\cdots h_t^{e_t}}) \quad \neq \quad 0.$$

In [5] we improved the algorithm as follows. We compute a CGS of the parametric saturation ideal $I' = I : (h_1 \cdots h_t)^\infty$ regarding $\bar{A}$ as parameters, then compute the multivariate Hermitian quadratic form $M^{I'}_{h_1^{e_1}\cdots h_t^{e_t}}$ for each $(e_1,\ldots,e_t) \in \{0,1\}^t$ and produce the equivalent quantifier free formula:

$$\sum_{(e_1,\ldots,e_t)\in\{0,1\}^t} \mathrm{sign}(M^{I'}_{h_1^{e_1}\cdots h_t^{e_t}}) \quad \neq \quad 0.$$

This formula is much simpler than the first one in general and we can have a program which is superior to any other existing implementations for many examples

containing many equalities as is reported in [5]. Our program is further improved by several techniques introduced in [6] and released as free software in [2]. By the fast CGS computation algorithm introduced in [8] together with improvements by the successive works we can now have a powerful implementation to compute CGSs. Nevertheless, there are many real QE problems such that we can compute a CGS of the associated parametric ideal I but cannot compute a CGS of the parametric saturation ideal $I : (h_1 \cdots h_t)^\infty$ since the computation of a saturation ideal is very heavy in general. As a result, there are some examples of real QE problems containing many equalities which cannot be handled by our program but can be handled by some other existing implementation.

In this talk, we study multivariate Hermitian quadratic forms introduced in [7] in more detail and show several facts which are proved by our group and especially important in a parametric polynomial ring. Using them we give an efficient method to compute the parametric saturation ideal $I : (h_1 \cdots h_t)^\infty$. It is implemented and embedded in our new real QE program released as free software in [3]. Our new program achieves a drastic improvement.

References

[1] Becker, E., Wörmann, T.: On the Trace Formula for Quadratic Forms. Proceedings of Recent Advances in Real Algebraic Geometry and Quadratic Forms, Contemporary Mathematics Vol.155, pp.271-291, American Mathematical Society, 1994.

[2] 2016 Version **CGSQE** Package: `http://www.rs.tus.ac.jp/fukasaku/software/CGSQE-20160509/`.

[3] 2017 Version **CGSQE** Package: `http://www.rs.tus.ac.jp/fukasaku/software/CGSQE-2017/`.

[4] Collins, G, E.: Quantifier elimination for real closed fields by cylindrical algebraic decomposition. Proceedings of Automata theory and formal languages, LNCS Vol.33, pp.134-183, Springer, 1975.

[5] Fukasaku, R., Iwane, H., Sato, Y: Real Quantifier Elimination by Computation of Comprehensive Gröbner Systems. Proceedings of International Symposium on Symbolic and Algebraic Computation, pp.173-180, ACM-Press, 2015.

[6] Fukasaku, R., Iwane, H., Sato, Y: On the Implementation of CGS Real QE. Proceedings of Mathematical Software - ICMS 2016 - 5th International Conference, LNCS Vol.9725, pp.165-172, Springer, 2016.

[7] Pedersen, P., Roy, M.-F., Szpirglas, A.: Counting real zeroes in the multivariate case. Proceedings of Effective Methods in Algebraic Geometry, Progress in Mathematics Vol.109, pp.203-224, Springer, 1993.

[8] Suzuki, A., Sato, Y.: A Simple Algorithm to Compute Comprehensive Gröbner Bases Using Gröbner Bases. Proceedings of International Symposium on Symbolic and Algebraic Computation, pp.326-331, ACM-Press, 2006.

[9] Weispfenning, V.: A New Approach to Quantifier Elimination for Real Algebra. Quantifier Elimination and Cylindrical Algebraic Decomposition, pp.376-392, Springer, 1998.

On continuity of the roots of a parametric zero dimensional multivariate polynomial ideal

Yosuke Sato[1] and Hiroshi Sekigawa[2]

[1] *Tokyo University of Science, Japan, ysato@rs.kagu.tus.ac.jp*

[2] *Tokyo University of Science, Japan, sekigawa@rs.tus.ac.jp*

Continuity of the roots of a parametric unary polynomial is easily obtained using Rouche's Theorem. For a system of multivariate parametric polynomials, however, it becomes a much subtler problem. The continuity property strongly depends on a generator of the corresponding parametric zero dimensional ideal. It seems that there have not been published any decisive paper on this problem.

In the talk, we show the following result **Theorem 1** which gives a sufficient condition of a generator of a parametric zero dimensional ideal for the continuity property of its roots. The notion of a comprehensive Gröbner system introduced in [4] and further developed by the successive works such as [1, 2, 3] plays a key role in our work.

In what follows, $\bar{A} = A_1, \ldots, A_m$ and $\bar{X} = X_1, \ldots, X_n$ denote variables, we consider $\bar{A}$ as parameters $\bar{X}$ as main variables. The symbol $\succ$ denotes an admissible term order on the set of all terms of $\bar{X}$, for a polynomial f in $\mathbb{Q}[\bar{A}, \bar{X}]$, $LM(f)$, $LT(f)$ and $LC(f)$ denote the leading monomial, the leading term and the leading coefficient of f respectively regarding f as a member of the polynomial ring over the coefficient ring $\mathbb{Q}[\bar{A}]$, i.e. $f \in (\mathbb{Q}[\bar{A}])[X]$.

Definition 1 Let S be an algebraically constructible subset of an affine space $\mathbb{C}^m$ for some natural number m. A finite set $\{\mathcal{S}_1, \ldots, \mathcal{S}_k\}$ of non-empty subsets of S is called an algebraic partition of S if it satisfies the following properties 1, 2 and 3:

1. $\cup_{i=1}^{k} \mathcal{S}_i = S$.
2. $\mathcal{S}_i \cap \mathcal{S}_j = \emptyset$ if $i \neq j$.
3. $\mathcal{S}_i$ is a locally closed set for each i, that is $\mathcal{S}_i = V_{\mathbb{C}}(I_1) \setminus V_{\mathbb{C}}(I_2)$ for the varieties $V_{\mathbb{C}}(I_1), V_{\mathbb{C}}(I_2)$ of some ideals I_1, I_2 of $\mathbb{Q}[\bar{A}]$.

Each $\mathcal{S}_i$ is called a segment.

Definition 2 Let S be an algebraically constructible subset of $\mathbb{C}^m$. For a finite subset F of $\mathbb{Q}[\bar{A}, \bar{X}]$, a finite set $\mathcal{G} = \{(\mathcal{S}_1, G_1), \ldots, (\mathcal{S}_k, G_k)\}$ satisfying the following properties 1, 2, 3 and 4 is called a comprehensive Gröbner system of F over S with parameters $\bar{A}$ w.r.t. $\succ$:

1. Each G_i is a finite subset of $\mathbb{Q}[\overline{A},\overline{X}]$.
2. $\{\mathcal{S}_1,\ldots,\mathcal{S}_k\}$ is an algebraic partition of S.
3. For each $\overline{c}\in\mathcal{S}_i$, $G_i(\overline{c})=\{g(\overline{c},\overline{X})|g(\overline{A},\overline{X})\in G_i\}$ is a Gröbner basis of the ideal $\langle F(\overline{c})\rangle$ in $\mathbb{C}[\overline{X}]$ w.r.t. $\succ$, where $F(\overline{c})=\{f(\overline{c},\overline{X})|f(\overline{A},\overline{X})\in F\}$.
4. For each $\overline{c}\in\mathcal{S}_i$, $LC(g)(\overline{c})\neq 0$ for any element g of G_i.

In addition, if each $G_i(\overline{c})$ is a minimal (reduced) Gröbner basis, $\mathcal{G}$ is said to be minimal (reduced). Being monic is not required. When $\mathcal{S}$ is the whole space $\mathbb{C}^m$, the words "over $\mathcal{S}$" is usually omitted.

Theorem 1 *Let $\mathcal{G}=\{(\mathcal{S}_1,G_1),\ldots,(\mathcal{S}_k,G_k)\}$ be a minimal comprehensive Gröbner system w.r.t. an arbitrary term order. If the ideal $\langle G_i(\overline{c})\rangle$ is zero dimensional for each $\overline{c}\in\mathcal{S}_i$, then the set of all roots of the system of the parametric polynomial equations $g(\overline{A},\overline{X})=0, g\in G_i$ is continuous in the segment $\mathcal{S}_i$ as a function of the parameters A.*

References

[1] Kapur, D., Sun, Y., Wang, D.: A New Algorithm for Computing Comprehensive Gröbner Systems. Proceedings of International Symposium on Symbolic and Algebraic Computation, pp.29-36, ACM-Press, 2010.

[2] Kurata, Y.: Improving Suzuki-Sato's CGS Algorithm by Using Stability of Gröbner Bases and Basic Manipulations for Efficient Implementation. Communications of the Japan Society for Symbolic and Algebraic Computation Vol.1, pp. 39-66, 2011.

[3] Nabeshima, K.: Stability Conditions of Monomial Bases and Comprehensive Gröbner systems. Proceedings of Computer Algebra in Scientific Computing, LNCS Vol.7442, pp.248-259, Springer, 2012

[4] Suzuki, A., Sato, Y.: A Simple Algorithm to Compute Comprehensive Gröbner Bases Using Gröbner Bases. Proceedings of International Symposium on Symbolic and Algebraic Computation, pp.326-331, ACM-Press, 2006

An algorithm for computing Grothendieck local residues I — shape basis case —

K. Ohara[1], S. Tajima[2]

[1] *Kanazawa University, Japan, ohara@se.kanazawa-u.ac.jp*
[2] *University of Tsukuba, Japan, tajima@math.tsukuba.ac.jp*

In this talk, we will give an algorithm for exactly computing Grothendieck local residues for rational n-forms of n variables under certain condition and show an implementation on a computer algebra system Risa/Asir. Grothendieck local residue is natural generalization of the well-known residue for complex functions of one variable and is defined as an integration of meromorphic n-form of complex n variables on a real n-cycle around an isolated common zero. Let us recall the analytic definition of Grothendieck local residues. (see [1] chapter 5 for detail.)

Definition. Denote by $\mathscr{O}(U)$ a ring of holomorphic functions on a ball $U \subset \mathbf{C}^n$. Suppose that $f_1(x),\ldots,f_n(x) \in \mathscr{O}(U)$ make regular sequence and have only one isolated common zero $\beta \in U$. Let $\Gamma(\beta)$ be a real n-cycle around β defined by $\Gamma(\beta) = \{x \in U \mid \|f_1(x)\| = \varepsilon,\ldots,\|f_n(x)\| = \varepsilon\}$ and oriented by $d(\arg f_1) \wedge \cdots \wedge d(\arg f_n) \geq 0$. Denote $\tau_F = (f_1(x)\cdots f_n(x))^{-1} dx_1 \wedge \cdots \wedge dx_n$, where $x = (x_1,\ldots,x_n)$. For any $\varphi(x) \in \mathscr{O}(U)$, the integration

$$\mathrm{Res}_\beta(\varphi(x)\tau_F) = \left(\frac{1}{2\pi\sqrt{-1}}\right)^n \int_{\Gamma(\beta)} \varphi(x)\tau_F$$

is called the *Grothendieck local residue* of meromorphic n-form $\varphi(x)\tau_F$.

Grothendieck local residue is a quite important concept in pure mathematics. However it is hard to directly evaluate them from the definition because of complicated geometric shape of the real n-cycle in $2n$-dimensional real space. The correspondence $\varphi \mapsto \mathrm{Res}_\beta(\varphi\tau_F)$ given by the local residue can be regarded as a distribution on $\mathscr{O}(U)$ and can be expressed by a linear partial differential operator. That is, there exists a linear partial differential operator $T_F = \sum_\alpha c_\alpha(x)\frac{\partial^\alpha}{\partial x^\alpha}$ determined by the regular sequence $F = \{f_1,\ldots,f_n\}$ such that $\mathrm{Res}_\beta(\varphi\tau_F) = (T_F \bullet \varphi)|_{x=\beta}$. Here "$\bullet$" is notation to express action by a differential operator to a function. Thus, the local residue can be evaluated if the operator T_F can be calculated. Our purpose is to develop new and effective method for exactly computing the operator T_F from the regular sequence under certain condition.

To treat the local residue using computer algebra system, we suppose that the regular sequence consists of polynomials. The set F generates a zero-dimensional

ideal I in $\mathbf{C}[x] = \mathbf{C}[x_1, \ldots, x_n]$. Then the local residue $\varphi \mapsto \mathrm{Res}_\beta(\varphi \tau_F)$ is determined by the algebraic local cohomology class $\sigma_F = \left[\frac{1}{f_1 \cdots f_n}\right] \in H^n_{[Z]}(\mathbf{C}[x])$. The linear partial differential operator T_F is called *Noether differential operator* with respect to the algebraic local cohomology class σ_F.

As it is well known, a polynomial ideal is decomposed to an intersection of primary ideals. Then the algebraic local cohomology class is also expressed as

$$\sigma_F = \sigma_{F,1} + \cdots + \sigma_{F,\lambda} + \cdots + \sigma_{F,N},$$

where the support Z_λ of $\sigma_{F,\lambda}$ coincides the zero set of corresponding primary component of I. Let $\beta \in Z_\lambda$ and $\varphi(x) \in \mathbf{C}[x]$. Since $\sigma_F dx = \sigma_{F,\lambda} dx$ on Z_λ, we have $\mathrm{Res}_\beta(\varphi\, \sigma_F dx) = \mathrm{Res}_\beta(\varphi\, \sigma_{F,\lambda} dx)$. Thus is allows to compute expression of the local residue on each irreducible components. We denote by $T_{F,\lambda}$ the corresponding Noether differential operator to the local residue $\varphi \mapsto \mathrm{Res}_\beta(\varphi\, \sigma_{F,\lambda} dx)$. Hence the set $\{(T_{F,\lambda}, Z_\lambda) \mid \lambda = 1, 2, \ldots, N\}$ gives an expression of the Noether differential operator T_F.

In this talk, we treat the special case that the primary ideal I_λ is expressed by shape bases. Our purpose is to determine the differential operator $T_{F,\lambda}$ from I_λ. We use two tools to solve this problem. One is Noether differential operator bases which describes a relation between I_λ and $\sqrt{I_\lambda}$. Another is a suitable subset of the annihilating ideal $\mathrm{Ann}_{D_n}(\sigma_{F,\lambda})$ of the algebraic local cohomology class σ_F. The annihilating ideal is a left ideal in the Weyl algebra D_n. So the cost of computation of $\mathrm{Ann}_{D_n}(\sigma_{F,\lambda})$ is high in general.

Under the shape base condition of primary ideals, we can explicitly construct Noether differential operator bases and suitable subset of $\mathrm{Ann}_{D_n}(\sigma_{F,\lambda})$ without Gröbner bases in Weyl algebra. Hence our algorithm is effective.

References

[1] P. Griffiths and J. Harris, *Principles of Algebraic Geometry*, Wiley Interscience, 1978.

[2] S. Tajima, On Noether differential operators attached to a zero-dimensional primary ideal — a shape basis case —, Finite or Infinite Dimensional Complex Analysis and Applications, 357–366, Kyushu Univ. Press, 2005.

[3] S. Tajima, Noether differential operators and Grothendieck Local Residues, RIMS Kôkyûroku **1432** (2005), 123–136. (in Japanese)

An implementation of the Lê -Teissier method for computing local Euler obstructions

Shinichi Tajima[1], Katsusuke Nabeshima[2]

[1] *University of Tsukuba, Tsukuba, Japan, tajima@math.tsukuba.ac.jp*
[2] *Tokushima University, Tokushima, Japan, nabeshima@tokushima-u.ac.jp*

In this talk, we present an algorithm for computing local Euler obstructions of a hypersurface with singular locus of positive dimension. The key ingredients of our approach are the concept of parametric local cohomology system and that of parametric polynomial systems.

The local Euler obstruction was introduced by R. D. MacPherson in a paper [6] publishied in 1974, as a key concept to prove the existence of Chern classes for possibly singular complex algebraic varieties, which was conjectured by P. Deligne and A. Grothendieck.

In 1973, M. Kashiwara published a short paper [4] on holonomic D-modules and presented an index theorem for a holonomc D-module. The index formula involves certain geometric invariants, called a local characteristics. Here we briefly recall the definition of the local characteristic.

Let X be an open neighborhood of the origin O in $\mathbb{C}^n$, Let S be an irreducible variety and let $S = \cup S_\alpha$ be a Whitney stratification of S. Let S_0 denote the open stratum of S.Let d_α be the dimension of S_α and let x_α be a point in S_α. Let x be a point in S. The local characteristic $c_x(S)$of S at x is defined inductively by the following formula:

$$c_x(S) = \Sigma_{S_\alpha \neq S_0} c_x(S_\alpha)\chi(U_\alpha \cap S_0 \cap Z_\alpha)$$

where $U_\alpha$is a sufficiently small ball with center x_α, Z_α is a $(d_\alpha + 1)$-codimensional linear plane in a general position in $\mathbb{C}^n$ sufficiently close to x_α and χ denotes the Euler characteristic. The sum is taken all over the strata S_α with $x \in \overline{S_\alpha}$.

These two concepts were independently introduced in different contexts, namely algebraic geometry and the theory of D-modules. It turened out in [3] surprisingly that the notion of local Euler obstruction and that of local characteristic are equivalents. The local Euler obstruction has been deeply investigated and utilised by everal authors, eapecially in the theory of singularities. Now it is known that the notion of local Euler obstruction can be defined in several different ways. Hereas, the computation of local Euler obstructions is quite difficult.

For the case where the hypersurface has an isolated singularity, we alredy have constructed in [8] an algorithm for computing local Euler obstructions. The key is the use of the concept of parametric local cohomology systems([9]).

We address in this talk the problem of construction of an algorithm for computing local Euler obstructions of hypersurfaces with possitive dimensional singular locus. For this purpose, we adopt the polar variety method developed by D. T. Lê and B. Teissier [5]. We show that the use of the parametric polynomial systems and that of parametric local cohomology systems arrows us to construct an algorithm of computing local Euler obstructions.

We present some examples of computation.

References

[1] J.-P. Brasslet, Local Euler obstruction, old and new, in Brazilian Topology Meeting (Rio Claro 1998) World Scientific, 2000, 140–147.

[2] J.-P. Brasslet, M. G. Grulha Jr, Local Euler obstruction, old and new II, London Math. Soc. Lecture Notes Ser. **380** (2010), 23–45.

[3] J. L. Brylinski, A. Dubson et M. Kashiwara, Formule de l'indice pour les Modules holonomes et obstruction d'Euler, *C. R. Acad. Sci. Paris*, série A **293** (1981), 573–576.

[4] M. Kashiwara, Index theorem for maximally overdetermined systems of linear differential equations, *Proc. Japan Acad.* **49** (1973), 803–804.

[5] Lê Duñg Tráng and B. Teissier, Variétés polaires locales et classes de Chern de variétés singulières, *Annals of Mhatematics* **114** (1981), 457—491.

[6] R. D. MacPherson, Chern class for singular algebraic varieties, *Ann. of Math.* **100** (1974), 423—432.

[7] K. Nabeshima, Comprehensive Gröbner bases in various domains, Doctoral Thesis, Johannes Kepler Universität Linz, Austria, 2007.

[8] K. Nabeshima and S. Tajima, Computing μ^*-sequences of hypersurface isolated singularities via parametric local cohomology systems, *Acta Mathematica Vietnamica*. **42**(2) (2017), 279–288.

[9] K. Nabeshima and S. Tajima, Algebraic local cohomology with parameters and parametric standard bases for zero-dimensional ideals, *Journal of Symbolic Computation.* **82** (2017), 91–122,

Computing integral numbers for a parametric ideal in a ring of convergent power series via comprehensive Gröbner systems

Katsusuke Nabeshima[1], Shinichi Tajima[2]

[1] *Tokushima University, Tokushima, Japan, nabeshima@tokushima-u.ac.jp*
[2] *University of Tsukuba, Tsukuba, Japan, tajima@math.tsukuba.ac.jp*

In this talk, first we present a new algorithm for computing integral numbers w.r.t. an ideal in a ring of convergent power series. Second, we likewise address the question of how to generalize the algorithms to parametric cases.

Let X be an open neighborhood of the origin O in $\mathbb{C}^n$, $\mathscr{O}_X$ the sheaf of holomorphic functions and $\mathscr{O}_{X,O}$ the stalk at the origin of $\mathscr{O}_X$.

Definition 1 *Let $\mathscr{I}$ be an ideal in the ring of convergent power series $\mathscr{O}_{X,O}$ (i.e., $\mathscr{O}_{X,O} = \mathbb{C}\{x_1, x_2, \ldots, x_n\}$). An element $h \in \mathscr{O}_{X,O}$ is said to be* **integral over** *$\mathscr{I}$ if there exists an integer r and elements $a_i \in \mathscr{I}^i$, $i = 1, 2, \ldots, r$, such that*

$$h^r + a_1 h^{r-1} + a_2 h^{r-2} + \cdots + a_{r-1} h + a_r = 0.$$

Such an equation is called **an equation of integral dependence of** *h* **over** *$\mathscr{I}$. The set of all elements that are integral over $\mathscr{I}$ is called* **the integral closure** *of $\mathscr{I}$.*

Definition 2 *Assume that $h \in \mathscr{O}_{X,O}$ is* **integral over** *$\mathscr{I}$. The smallest number r that satisfies*

$$h^r + a_1 h^{r-1} + a_2 h^{r-2} + \cdots + a_{r-1} h + a_r = 0,$$

is said to be **integral number of** *h w.r.t. $\mathscr{I}$ where $a_i \in \mathscr{I}^i$, $i = 1, 2, \ldots, r$.*

Let F be a set of polynomials $f_1, f_2, \ldots, f_s$ in $\mathbb{C}[x_1, \ldots, x_n]$ such that $\{x \in X \mid f_1(x) = f_2(x) = \cdots = f_s(x) = 0\} = \{O\}$. Let $\mathscr{I}_O$ be the ideal generated by F in the ring of convergent power series $\mathscr{O}_{X,O}$ and $h \in \mathbb{C}[x_1, \ldots, x_n]$.

The first aim of this talk is giving a new algorithm for computing the integral number of h w.r.t. $\mathscr{I}_O$. The second aim is extending the algorithm to parametric cases by using comprehensive Gröbner systems.

Let ℓ be the integral number of h w.r.t. $\mathscr{I}_O$. Then,

$$\begin{aligned} h^\ell &+ a_1 h^{\ell-1} + a_2 h^{\ell-2} + \cdots + a_{\ell-1} h + a_\ell = 0 \\ h^\ell &= -a_1 h^{\ell-1} - a_2 h^{\ell-2} - \cdots - a_{\ell-1} h - a_\ell, \end{aligned}$$

where $a_i \in \mathscr{I}_O^i$, $1 \leq i \leq \ell$. That is,

$$h^\ell \in (h^{\ell-1}\mathscr{I}_O + h^{\ell-2}\mathscr{I}_O^2 + \cdots + \mathscr{I}_O^\ell).$$

Therefore, solving the integral number of h w.r.t. $\mathscr{I}_O$ is equivalent to solving the ideal membership problem in the ring of convergent power series.

We have the following lemma for solving ideal membership problems in the ring of convergent power series.

Lemma 3 *Let q be a polynomial in $\mathbb{C}[x_1,\ldots,x_n]$ and I be an ideal generated by F in the polynomial ring $\mathbb{C}[x_1,\ldots,x_n]$. Then, $q \in \mathscr{I}_O$ in $\mathscr{O}_{X,O}$ if and only if there exists a polynomial $g \in I : \langle q \rangle$ such that $g \notin \mathfrak{m}$, where $I : \langle q \rangle$ is the ideal quotient in $\mathbb{C}[x_1,\ldots,x_n]$ and $\mathfrak{m} = \langle x_1, x_2, \ldots, x_n \rangle$ is the maximal ideal in $\mathscr{O}_{X,O}$.*

As an algorithm for computing a basis of an ideal quotient is based on a Gröbner basis computation, thus we can construct an algorithm for computing the integral number of h w.r.t. $\mathscr{I}_O$ via Gröbner basis.

If h or $f_1,\ldots,f_s$ has parameters, then we need a comprehensive Gröbner system to solve (parametric) ideal membership problems, namely, we need it to compute a basis of an ideal quotient. In parametric cases, the ideal quotient algorithm is more complicated than the non-parametric ones. In fact, an extended Gröbner basis algorithm is required to obtain a basis of ideal quotient. In this talk, we give the detail of the algorithm and demonstrations of our implementation.

Let $h = ay^4z + z^4$ and $f = x^2z + yz^2 + y^6 + ay^4z + z^4$ where x, y, z are variables and a is a parameters. Our implementation outputs the integral numbers of h w.r.t. $\langle \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z} \rangle$ in $\mathscr{O}_{X,O}$, as follows.

- If $a \neq 0$, then the integral number is 2.
- If $a = 0$, then the integral number is 1.

References

[1] D. Kapur, Y. Sun and D. Wang, A new algorithm for computing comprehensive Gröbner systems. *Proc. ISSAC2010*, pp. 29–36. ACM, (2010).

[2] K. Nabeshima, Stability Conditions of monomial bases and comprehensive Gröbner systems, Lecture Notes in Computer Science, **7442**, pp.248–259, Springer, (2012).

[3] K. Nabeshima and S. Tajima, *Solving extended ideal membership problems in rings of convergent power series via Gröbner bases*, Lecture Notes in Computer Science, **9582**, pp.252-267, Sprinbger, (2016).

[4] I. Swanson and C. Huneke, *Integral Closure of Ideals, Rings, and Modules*, Cambridge University Press, (2006).

Session 13

Computer Algebra in Image Processing

Session chairs:

Erick Fredj
Department of Computer Science, Jerusalem College of Technology, Israel

Moti Reif
Department of Computer Science, Jerusalem College of Technology, Israel

David Zeitoun
Department of Mathematics, Orot Israel College, Elkana, Israel

Breast Cancer Risk Estimation based on Machine Learning Methods for Computerized Assessment of Breast Composition in Digital Mammograms

Ya'akov Mandelbaum[1], Amitay Stein[2], Yitzhak Yitzhaky[2], Isaac Leichter[1]

1. Dept. of Applied Physics, Lev Academic Center, Jerusalem, Israel
2. Dept. of Electro-Optics Engineering, Ben Gurion University, Beer-Sheva, Israel

Objective:

The aim of the study is to develop a computer algorithm to automatically calculate the percentage of glandular tissue in a mammogram, making the results independent of the estimation of the interpreting radiologist.

Background:

A few studies have demonstrated a relationship between breast composition, tissue density in particular, and the risk of breast cancer [1]. Breast tissue which appears brighter on the mammogram is considered dense breast, and is due to a high percentage of glandular tissue. By contrast a high percentage of adipose (fatty) tissue in the breast reduces the breast density, and the resulting mammogram brightness. To date, the estimation of the percentage of glandular tissue is based on the subjective evaluation of the radiologist who must visually estimate the percentage of “bright areas" (glandular tissue) relative to the total breast image under consideration. This estimation is subjective and known to be imprecise and not consistent.

A typical mammography study contains four standard images, taken from different angles. In the MLO views the pectoral muscle, extraneous to the breast tissue, occupies a significant portion of the image. Any computerized analysis must start with the removal of the pectoral muscle from the image.

Material and Methods

The calculation of the percentage of glandular tissue was accomplished in two stages. First the subtraction of the pectoral muscle from the mammographic image was accomplished using a thresholding operation which creates a black and white

image in which the pectoral muscles appears differentiated from the adjacent breast tissue. The optimal threshold is determined by an algorithm which combines morphological methods with empirical results.

Following segmentation of the pectoral muscle, the glandular tissue is identified by classification of the mammographic images into 3 classes based on the characteristics of the histogram as well as texture analysis. For one class the glandular tissue was segmented using Seed Region Growing (SRG). For the other two classes, a threshold value was computed using a multivariate linear regression model, correlating histogram characteristics to an empirically specified threshold, determined by participating medical experts. Following identification of the glandular tissue, its area by percentage of the total breast tissue is computed.

Results:

The resulting algorithm was developed based on a training set, as described. Testing was performing on a verification set of 160 mammogram images. The results were compared to the area percentage computed based on the evaluation of independent radiologists, who manually defined the glandular tissue on the image. A high correlation of 0.92 was found between the results of the algorithm and those of the radiologists.

Conclusion:

The computerized algorithm developed presents an objective and systematic method to quantitatively evaluate the tissue density of breast tissue and thus improve the diagnostic accuracy of mammography.

Use of coordinates systems for 3D plot of discontinuous functions

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

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

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

The study of functions of two real variables can be supported by visualization using a Computer Algebra System (CAS).Historically, contour plots were the first type of graphical representations. With the development of scientific computing, 3D plots were introduced and plotting the graph of a two-variable function has been made possible, including parametric plotting and implicit plotting. In most of the CAS such as MATLAB, Maple, Mathematica, the 3D plot may be builded using local coordinates systems and linear interpolation of the function using local parameters.

When the function is continuous, the uniform convergence of the approximated function to the function is proved by Bernstein Theorem [5].Then the 3D plot is independent of the type of local coordinate system. Therefore, the same 3D plot is generated by different local coordinates; see [2].

However, in a neighborhood of a discontinuity, Bernstein Theorem fails and the 3D plot is strongly dependant on the type of local coordinates chosen for the 3D plot.

In this present paper, we analyze the various aspects of the 3D plot created by different local coordinates. The study focuses on functions of the type $f(x,y) = \frac{P(x,y)}{Q(x,y)}$ where $P(x,y)$ and $Q(x,y)$ are polynomials of degree 2.

We distinguish different types of discontinuities:

1. $Q(x,y)$ is a linear function;
2. $Q(x,y)$ is a quadratic function;
3. $Q(x,y)$ contains linear and quadratic functions.

The choice of an adequate coordinate system is required before generating a 3D plot because of two main problems:

1. A non suitable choice of local coordinates may yield an inaccurate plot. In this case, the discretization of the function on the local coordinates miss the discontinuity points or lines.
2. Non accurate erratic behavior along the discontinuities appears.

3. Regular plots may be obtained when geodesics on the surface $Q(x,y) = k$ are used.

4. Multiple discontinuities are also analyzed. This analysis is based on image processing algorithm used for curve extractions.

Finally, a comparison of some different plotting software such as MATLAB, Maple, K3Dsurf around the choice of local coordinate systems, will be presented. We will focus on the application of image processing for the visualization of the discontinuities surfaces.

References

[1] D.G. Zeitoun and T.Danna- Picard: *Zooming algorithms for accurate plotting of two real variables ACA conference 2015.*

[2] Zeitoun, D.G. and Dana Picard, Th.: Accurate visualization of graphs of functions of two real variables, Int. J. of Comput. and Math. Sc. 4 (1), 1-11 (2010).

[3] Zeitoun, D.G., Laible, J.P. and Pinder, G.F.: An Iterative Penalty Method for the Least Squares Solution of Boundary Value Problems, Numerical Methods for P.D.E. **13**, 257-281 (1997).

[4] Botsch M, Kobbelt L.: Resampling feature and blend regions in polygonal meshes for surface anti-aliasing. In: Proceedings of Eurographics (01), 402–10 (2001).

[5] Achieser N.I. Theory of Approximation.(1951) New York: Frederick Ungar Publishing Co.

CAS for Simulating Modern Art: Enforcing "Fractal" Structure

D. Walker, J. Benjamin, T. Mylläri, A.Mylläri

St. George's University, Grenada, West Indies {amyllari}@sgu.edu

We experiment in emulating modern art with CASs. We start with grey-scale image and enforce self-similar ("fractal") structure on it. If one looks on the result close-up, only a collage of the same image is observed, but when one moves away, the real picture reveals itself.

At the core of this project lies the concept of fractals, a phenomena that is seen throughout nature in everything from the cauliflower to the coastline paradox. The seemingly hidden intricacies can add complexity to even the most basic structures. Mosaics and impressionisms are excellent examples of subtle complexities in imagery, at a glance, a given image can appear as one unit, yet when scrutinized up close can be seen as comprising of many distinct subunits. This project utilizes computer algebra systems to create imagery that imitates fractals in a finite manner.

Images constructed as a collage have a long history in arts, e.g. a cycle dedicated to the four seasons by Giuseppe Arcimboldo (1526-1593) in Kunsthistorisches Museum, Vienna, Austria. As a more fresh example one can mention Salvador Dali's Painting "Gala Contemplating the Mediterranean Sea which at a distance of 20 meters is transformed into the portrait of Abraham Lincoln (Homage to Rothko)" (1976). From the other side, fractal analysis is used as a tool for authentication of Jackson Pollock paintings [1]. Recent studies of the fractality of the boundaries of the Rorschach Blots shows that the number of images perceived when observing the blots decreases with increasing of fractal dimension [2].

Here, we emulate "fractal" structure by enforcing self-similarity into the image. We start with a grey-scale image and make two low-resolution images of it, one to be used for the collage, another as a base for the collage. Then we divide the base image into blocs (2x3) or (3x4) depending on the scale of the original image and replace these blocks by the small copy of the original image with adjusted brightness and contrast. The resulting image looks like a collage (repetition) of the same image when observed close-up, but reveals original image when seen from far away. Some examples are given in Figures 1-4.

References

[1] Coddington J., Elton J., Rockmore D., and Wang Y., *Multifractal analysis and authentication of Jackson Pollock paintings*, in *SPIE Proceedings Computer Image Analysis in the Study of*

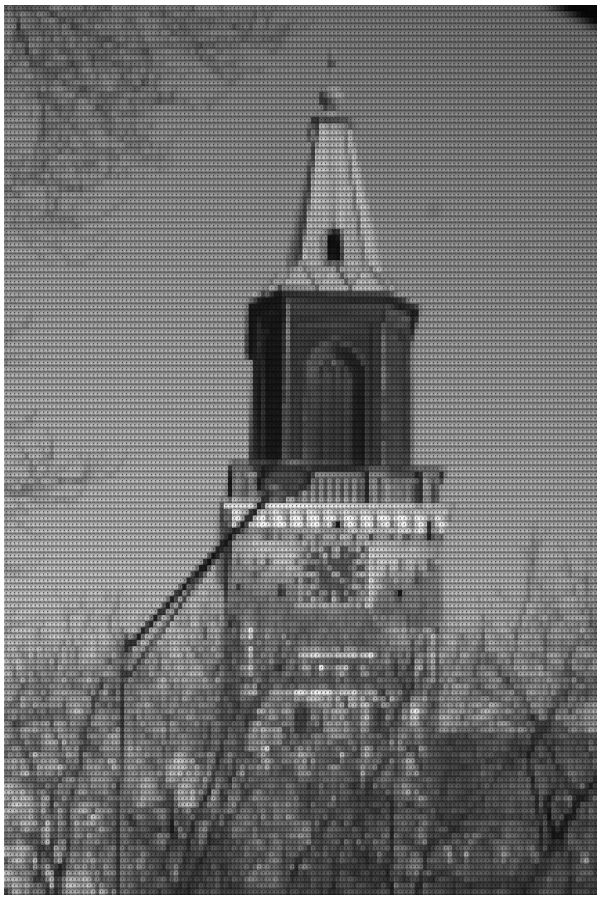


Figure 1:

Art (SPIE-2008), Bellingham, WA, ed. D. G. Stork, J. Coddington, **6810**, pp. 68100F (2008)

[2] Taylor RP, Martin TP, Montgomery RD, Smith JH, Micolich AP, Boydston C, et al. *Seeing shapes in seemingly random spatial patterns: Fractal analysis of Rorschach inkblots*, PLoS ONE **12**(2): e0171289 (2017).

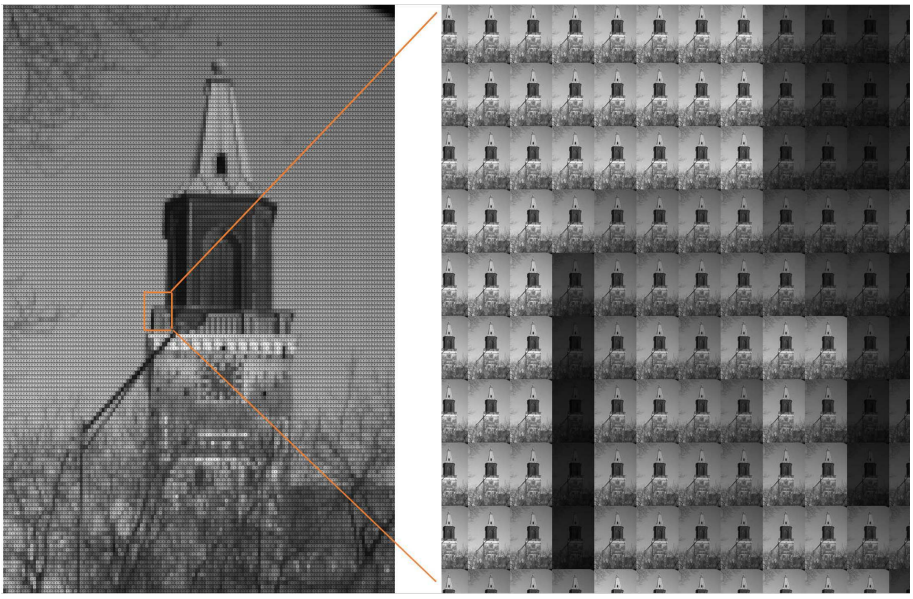


Figure 2:

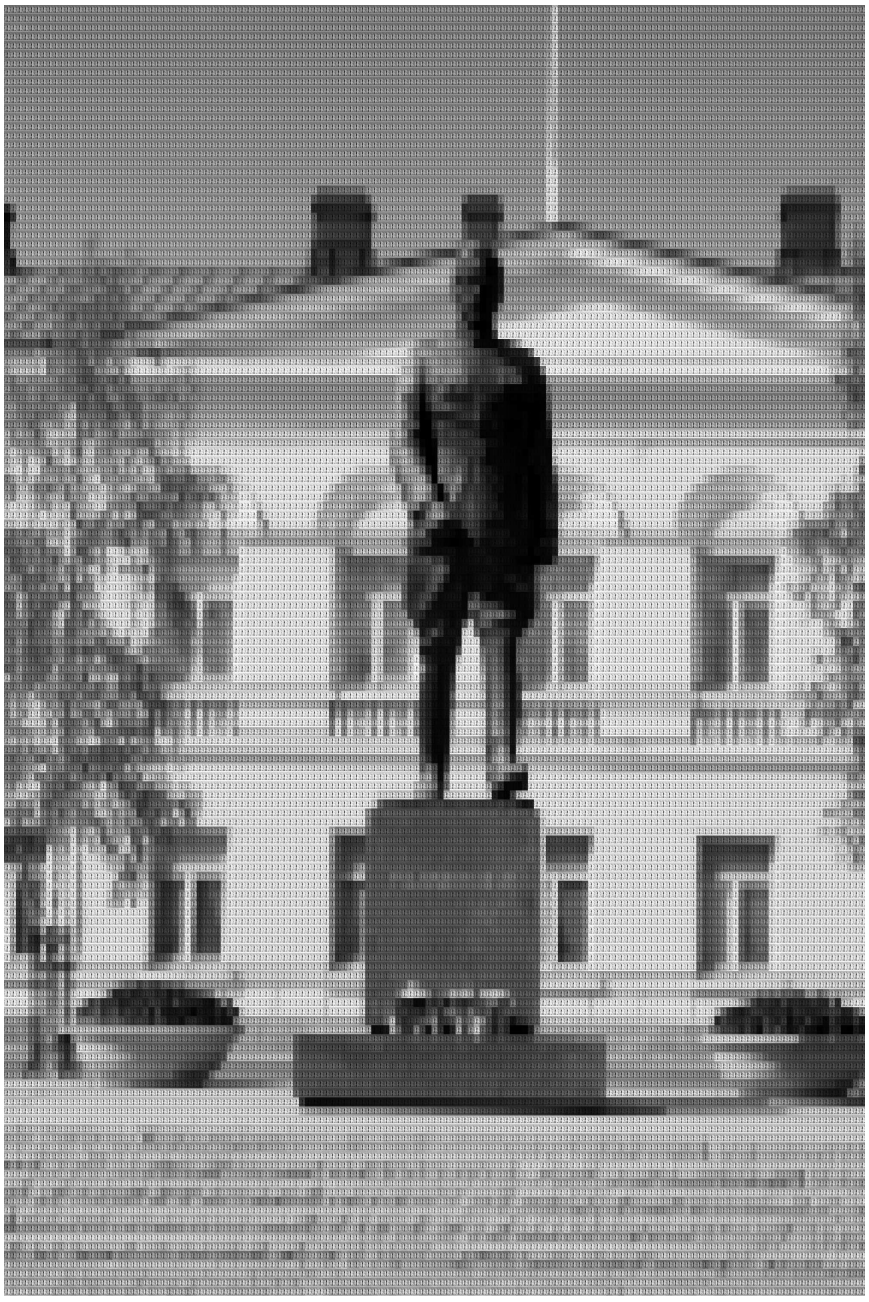


Figure 3:

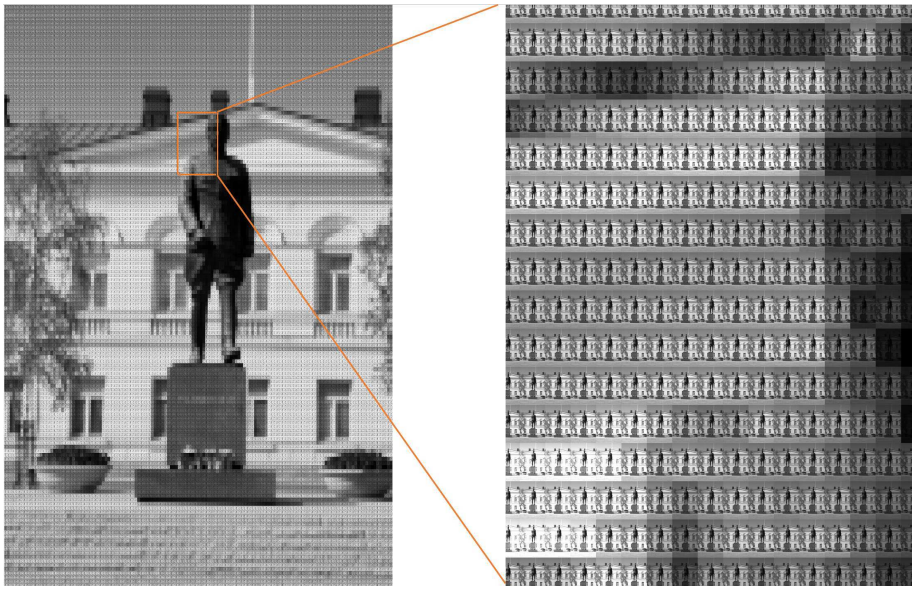


Figure 4:

Evolution of the olive pit from the time of the Mishna to present time, based on 3D image processing techniques.

Fredj Erick[*(a)] *and Friedman Naftali*[(a)]

(a) Jerusalem College of Technology, Dept. of Computer Science, Jerusalem.

Abstract

A seemingly innocuous question in the realm of *Halakha* raises challenges in other areas, spanning the disciplines of history, botany, mathematics and computer sciences. There is a known discrepancy between the *Halachic* measurement units of length and volume and those known to us today, which has led to the opinions that some changes have occurred in the physical world, even if the possibility of inner contradictions within *halachic* definitions are disregarded. Specifically, there may be a contradiction between *Hazal's* measurements of olives and modern measurements, with the result that the *halakhic* "*kazayit*" differs from the size of the olive. Assuming the discussions of *Hazal* actually referenced "medium olives" during that era, it is imperative to identify the type and average size of this olive. Several dominant olives have been identified in the Mediterranean area. Additionally, some archeological digs have revealed olive pits dating to the time of *Hazal*. Correlating these pits with olive pits prevalent today might give us a clue, though each pit needs to be identified as a certain specimen in order to measure the relation between modern olives and olives of the past. A series of verifications should clarify the classification issue. The research we present includes manual tests to check several characteristics of the olive pits and identify them based on this classification. State of the art three-dimensional scanning technology allows digitization of data such as these olive pits, and classification tests can be done much more quickly and with greater accuracy.

Session 14

Computer Algebra in Algebraic Graph Theory

Session chairs:

Roman Nedela
University of West Bohemia, Plzeň, Czech Republic

Sven Reichard
TU Dresden, Dresden, Germany

Cayley graphs based on octonions, and their implementation in MAGMA

X. Dahan[1]

[1] *Ochanomizu University, Japan, dahan.xavier@ocha.ac.jp, xdahan@gmail.com*

Cayley graphs occupy an important part in algebraic graph theory. Beyond the classical construction that requires groups, it is less known that *quasi-groups* are sufficient [4], *e.g.* to obtain regular graphs (under very mild assumptions). We have constructed new infinite families of regular Cayley graphs based on *Moufang loops* [1]. These loops (non-associative counterpart of a group) arise naturally as the multiplicative subloops $\mathbb{O}^\star(\mathbb{F}_q)$ of octonion algebras over a finite field $\mathbb{F}_q$. There are striking analogies between quotients of these loops by their center $\mathscr{Z}$, denoted $\mathbb{O}^\star(\mathbb{F}_q)/\mathscr{Z}$, and the groups $PGL_2(\mathbb{F}_q)$. This stems for the fact that the 2-by-2 matrices over $\mathbb{F}_p$ (p an odd prime) are isomorphic to some quaternion algebras $\mathbb{H}(\mathbb{F}_p)$, and that octonions are *doubling* algebras of quaternions.

While Cayley graphs on $PSL_2(\mathbb{F}_p)$ have been extensively studied with respect to many aspects, their non-associative counterparts much less (besides [2], we are not aware of concrete examples of construction of Cayley graphs on loops). The construction we have provided [1] is inspired by the famous Ramanujan graphs of Lubotzky-Phillips-Sarnak (LPS) [3]: first construct a free group on some generators of the integral octonions (say over $\mathbb{Z}$) of given norm p, yielding an infinite regular tree, and by reducing modulo another prime q, to obtain finite quotients of the infinite regular tree.

- For each odd prime p, there is a distinguished family $\mathscr{P}(p) \subset \mathbb{O}(\mathbb{Z})$ of p^3+1 integral octonions of norm p whose Cayley graph is an infinite regular tree.
- for each prime $q > p$, let $\mathscr{S}_{p,q}$ be the canonical image of $\mathscr{P}(p)$ in $\mathbb{O}^\star(\mathbb{F}_q)/\mathscr{Z}$: this yields a Cayley graph

$$\mathscr{X}_{p,q} = \mathscr{C}ay(\mathscr{S}_{p,q}, \mathbb{O}^\star(\mathbb{F}_q)/\mathscr{Z}), \tag{1}$$

  of degree p^3+1, connected bipartite if $\left(\frac{p}{q}\right) = -1$ and non-bipartite with two connected components of same order otherwise. The order is $|\mathbb{O}^\star(\mathbb{F}_q)/\mathscr{Z}| = q^7 - q^3$.

Despite these analogies with the LPS Ramanujan graphs, studying the properties of the graphs $\mathscr{X}_{p,q}$ is much more difficult than for Cayley graphs on $PSL_2(\mathbb{F}_p)$. We conjecture that:

1. the graphs $\mathscr{X}_{p,q}$ are not vertex-transitive
2. the bipartite graphs $\mathscr{X}_{p,q}$ are semi-symmetric (edge-transitive, non vertex transitive).

However describing even a single non-trivial automorphism is not easy (note that the automorphism obtained by the multiplication by a group element in Cayley graphs on groups does not exist in Cayley graphs on loops). The sole construction of non-vertex transitive Cayley graphs on Moufang loops is in [2] where the authors used the notion of regular maps, thereby constraining to degree 3 regular graphs.

The investigation of the properties of the graphs $\mathscr{X}_{p,q}$ has motivated an implementation [1] in MAGMA; And in order to check the implementation, of the LPS Ramanujan graphs as well for which theoretical results are known and thus can be verified. Due the rapidly increasing order/size of these graphs when q or p grows, it becomes quickly impossible to build or even store the whole adjacency table of the graphs. We could compute however the second largest eigenvalue using the power method, and the girth (they are not Ramanujan graphs, neither have they large girth as the LPS Ramanujan graphs). However, these computations support the conjecture above (the girth is not uniform as in vertex-transitive graphs).

References

[1] X. Dahan and J.-P. Tillich. On the computation of the second largest eigenvalue and of the girth of Cayley graphs based on octonions and quaternions, 2016. *Preprint (31 pages)*. `http://xdahan.sakura.ne.jp/preprint/octonionGraphs.pdf`.

[2] T.S. Griggs, J. Širáň, and R.B. Richter. Graphs obtained from Moufang loops and regular maps. *Journal of Graph Theory*, 70(4):427–434, 2012.

[3] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[4] E. Mwambene. Cayley graphs on left quasi-groups and groupoids representing k-generalised Petersen graphs. *Discrete Math.*, 309(8):2544–2547, 2009.

[1] See the web-page `http://xdahan.sakura.ne.jp/Package/graph.html` for some brief instructions and to download the source code

A Collection of Procedures for Working with Directed Strongly Regular Graphs in GAP

Š. Gyürki[1]

[1] *Matej Bel University, Banská Bystrica, Slovakia, stefan.gyurki@umb.sk*

We report about a collection of routines written in computer algebra system GAP [2] which allow efficient working with directed strongly regular graphs. Since the main objects of interest in algebraic graph theory are highly symmetric graphs, strongly regular graphs are playing a central role in this area. One of their possible generalization for directed graphs was given by Duval in 1988, see [1]. These objects started to receive more and more attention recently, therefore we developed a package of routines in GAP in order to make easier working with them. Several successful experimentations have been already reported (see [3, 4]), while other computer results are still waiting for theoretical generalizations.

A *directed strongly regular graph* (DSRG) with parameters (n,k,t,λ,μ) is a regular directed graph on n vertices with valency k, such that every vertex is incident with t undirected edges, and the number of paths of length 2 directed from a vertex x to another vertex y is λ, if there is an arc from x to y, and μ otherwise. In particular, a DSRG with $t = k$ is an SRG, and a DSRG with $t = 0$ is a doubly regular tournament. The adjacency matrix $A = A(\Gamma)$ of a DSRG with parameters (n,k,t,λ,μ), satisfies $AJ = JA = kJ$ and

$$A^2 = tI + \lambda A + \mu(J - I - A). \tag{1}$$

Dealing with a DSRG always provides a challenge and poses a lot of questions:

- Does it contain subgraphs with nice properties?
- Can we interpret and generalize the idea of its construction?
- What are its connections to other combinatorial structures?

Answering these questions can be made easier with a few routine inspections which can be left as a job for a computer.

IsDSRG: Checks whether a zero-one matrix A corresponds to a DSRG, or not. In the first step it determines the candidates for the parameters t,λ,μ, after that checks equation (1).

AllInducedDSRGs, AllQuotientDSRGs: For a given graph it computes the system of imprimitivity of its group of automorphisms and checks for all block systems, whether there appear DSRGs among the graphs induced by the blocks, or on the quotient graphs with respect to blocks.

DSRGfromColorGraph: Starting from a color graph it checks all the possibilities for creating digraphs as union of colors, up to algebraic automorphisms. It uses the SetOrbit package written by Pech and Reichard, see [5, 6].

WLClosureOfDSRG: It computes the smallest coherent configuration, which contains the given DSRG. It is based on Matan Ziv-Av's procedure for computing WL-closure (Weisfeiler-Leman closure) of a graph [7].

It is needless to mention the importance of the procedure IsDSRG. Using of procedures AllInducedDSRGs and AllQuotientDSRGs resulted in the understanding of some bigger DSRGs. Their computer-free interpretation on the theoretical level lead to the results published in [4], where we report about a construction which creates bigger DSRGs from smaller ones under certain conditions. The procedure DSRGfromColorGraph played the key role in the discovery of DSRGs as union of relations in association schemes. The results are reported in [3].

Acknowledgements

The author gratefully acknowledges the contribution of the Scientific Grant Agency of Slovak Republic under the grant VEGA 1/0988/16 and the contribution of the Slovak Research and Development Agency under the projects APVV-0136-12 and APVV-0220-15. The author is very grateful to Misha Klin, Sven Reichard and Matan Ziv-Av for helpful communications on various topics from computer algebra systems and algebraic graph theory.

References

[1] A.M. Duval, *A directed graph version of strongly regular graphs*, J. Combin. Th. A **47**, pp. 71–100 (1988).

[2] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.8.7*; 2017, (`http://www.gap-system.org`).

[3] Š. Gyürki, M. Klin, *Sporadic examples of directed strongly regular graphs obtained by computer algebra experimentation*, in Gerdt, V.P. (ed.) et al., Computer algebra in scientific computing. CASC 2014, Proceedings. Berlin: Springer. Lecture Notes in Computer Science **8660**, pp. 155–170 (2014).

[4] Š. Gyürki, *Infinite families of directed strongly regular graphs using equitable partitions*, Discrete Math. **339** pp. 2970–2986 (2016).

[5] Ch. Pech, S. Reichard, *The* SetOrbit *package for* GAP, (accessed April 2017), `http://www.math.tu-dresden.de/~pech`.

[6] Ch. Pech, S. Reichard, *Enumerating set orbits*. in: M. Klin et al., Algorithmic Algebraic Combinatorics and Gröbner Bases, Springer, Berlin, Heidelberg pp. 137–150 (2009).

[7] M. Ziv-Av, *Personal communication*, (2017).

Classification of discrete group actions on Riemann surfaces of higher genera

Ján Karabáš[1,2], Roman Nedela[1]

[1] *New Technologies for Information Society, University of West Bohemia, Pilsen, Czech republic,*
[2] *Department of Computer Sciences, Faculty of Natural Sciences, Matej Bel University, Banská Bystrica, Slovakia,* karabas@savbb.sk

Discrete actions of finite groups on surfaces appears in many situations in numerous branches of mathematics, cryptography, quantum physics, and many other fields of science. In topological graph theory they can be used to derive lists of highly symmetrical (oriented) maps of fixed genus: regular maps, vertex-transitive maps, Cayley maps, or edge-transitive maps. In particular, the classification of actions of cyclic groups is essential for solving enumeration problems of combinatorial objects, i.e. maps, graphs and others.

The classification of groups acting on the sphere is a classical part of crystallography. In case of torus the situation is in principle known, though there are infinitely many group actions. The problem of classification of discrete actions of groups on orientable surfaces of genera $g \geq 2$ is nowadays challenge. Due to Hurwitz bound there are just finitely many finite groups acting on a surface of given genus $g \geq 2$. The solution to the problem turned to be "realisable": the classification can be done with help of computer algebra systems. Published lists of actions (without help of CAS's) go up to genus five [1, 3, 5].

Using MAGMA [2] we already derived the list of actions of discrete groups on surfaces of genus $2 \leq g \leq 21$ [4]. We shall discuss the details of the procedure, further improvements and applications.

References

[1] O. V. Bogopolski, *Classifying the actions of finite groups on orientable surfaces of genus* 4 *[translation of proceedings of the Institute of Mathematics, 30 (Russian), 48–69, Izdat. Ross. Akad. Nauk, Sibirsk. Otdel., Inst. Mat., Novosibirsk, 1996]*, Siberian Adv. Math. **7**, no. 4, 9–38, Siberian Advances in Mathematics (1997).

[2] W. Bosma, J. Cannon, C. Fieker, and A. Steel, *Handbook of Magma functions*, Version 2.22, Sydney, 2016.

[3] S. A. Broughton, *Classifying finite group actions on surfaces of low genus*, J. Pure Appl. Algebra **69**, no. 3, 233–270 (1991).

[4] J. Karabáš, *Actions of finite groups on Riemann surfaces of higher genera*, http://www.savbb.sk/~karabas/finacts.html, 2013.

[5] A. Kuribayashi and H. Kimura, *Automorphism groups of compact Riemann surfaces of genus five*, J. Algebra **134**, no. 1, 80–103 (1990).

A physics perspective on Algebraic Graph Theory (AGT)

M. Kagan[1]

[1] *Pennsylvania State University, Abington, PA, USA, mak411@psu.edu*

Our knowledge and intuition about electrical circuits can provide an interesting insight on AGT. One of the prime concepts adopted from electric circuits is the equivalent resistance, $R_{\rm eq}$ (*resistance distance* in [1]). A particularly simple expresssion for $R_{\rm eq}$, recently obtained in [2], yields a convenient tool to

- Investigate and make analytical statements about connectivity of graphs.
- Count the number of spanning trees and forests of certain type.
- Compute the resistance distance for generic graphs of finite size, as well as for infinite or large graphs (with explicit dependance on the graph size) that exhibit some symmetry or pattern [5].
- Allow for complex valued edge weights by considering the complex impedance of AC-circuits. The expression for the equivalent impedance readily allows to investigate the resonance phenomena in AC-circuits.
- Given the analogy between electric circuits and random walks on graphs [3], one can readily obtain the corresponing quantities of interest for the latter, such as, for instance, the *escape probability*.

Consider a graph G with n vertices and designate the edge conductance (inverse resistance) between vertices i and j as $\sigma_{ij} = 1/R_{ij} = \sigma_{ji}$. Without loss of generality, assume that every vertex is connected to every other vertex. If, in reality, some vertices are not connected by an edge, we simply put the corresponding edge conductance to zero. The weighted Laplacian (Kirchhoff) matrix for G is given by

$$L_{ij} = -\sigma_{ij} \quad \text{for} \quad i \neq j, \quad \text{and} \quad L_{ii} = \sum_{j=1}^{n} \sigma_{ij}. \tag{1}$$

The equivalent resistance between vertices i and j can be written as [2]

$$R_{\rm eq}(i,j) = \frac{\Delta''_{ij}}{\Delta'}, \tag{2}$$

where Δ' is (any) co-factor of the Laplacian matrix and Δ''_{ij} the determinant of L with rows and columns i and j removed. These determinants have several key

properties. Both Δ' and Δ''_{ij} are polynomials (of degree $n-1$ and $n-2$ respectively) in the edge conductances σ_{ij} and contain only positive monomials (n^{n-2} and $2n^{n-3}$ respectively) which are linear in each particular σ_{ij}.

Furthermore, the set of edges appearing in each such monomial of Δ' represents a spanning tree of graph G. Putting each non-zero σ_{ij} to 1, yields the Kirchhoff theorem ($\Delta' =$ number of spanning trees). The set of edges in each monomial of Δ''_{ij} represents a *forest* of two trees in G: one connected to vertex i and the other one to vertex j. (One of the trees to be just vertex i or just vertex j.) By putting each non-zero σ_{ij} to 1, Δ''_{ij} would count the number of ways to have all vertices of G connected (through a path) to either i or j. We can define analogous determinants Δ'''_{ijk} and so on, by removing from L the rows and columns i, j, and k and so on. Δ'''_{ijk} correspond to forests with trees connecting all vertices in G to either i, j, or k.

In the physics (electric) context, the two special vertices i and j in Δ''_{ij} are understood as the terminals of the voltage source (battery). If $\Delta''_{ij} = 0$, it follows from the Kirchhoff's vertex equations [4] that some vertex potentials cannot be determined, which implies that there are components of G that are not connected to the battery. Moreover, the multiplicity of zero eigenvalue in Δ''_{ij} gives the number of such disconnected components. Since any circuit with finite (or zero) values of edge conductance must have a finite value of equivalent conductance, it follows from Eq. (2) that if $\Delta''_{ij} = 0$ then so is Δ'. Also on the grounds of equivalent conductance, if $\Delta''_{ij} \neq 0$, G is connected (disconnected) if and only if $\Delta' \neq 0$ ($\Delta' = 0$).

Finally, it can be shown that

$$\Delta''_{ij} = \frac{\partial \Delta'}{\partial \sigma_{ij}}, \quad \Longrightarrow \quad R_{\rm eq}(i,j) = \frac{\partial \ln \Delta'}{\partial \sigma_{ij}}. \tag{3}$$

Thus for many analytical purposes it is sufficient to know Δ' as a function of the edge conductances σ_{ij}. For relatively small graphs, such explicit expressions can be obtained using widely avilable mathematical packages.

References

[1] D. J. Klein and M. Randić, *Resistance distance*, J. Math. Chem., Vol **12**, pp. 81-95 (1993).

[2] M. Kagan, *On equivalent resistance of electrical circuits*, Am. J. Phys. **83**, pp. 53-63 (2015).

[3] P. Doyle and L. Snell, *Random Walks and Electric Networks*, (Mathematical Assn of America, USA, 1984).

[4] Gustav Kirchhoff, Ann. Phys. Chem. **72**, pp. 497-508 (1847) [English translation by O'Toole JB: Kirchhoff G (1958) *On the Solution of the Equations Obtained from the Investigation of the Linear Distribution of Galvanic Currents. IRE Trans Circuit Theory CT5:4–8.*]

[5] M. Kagan and X. Wang, *Infinite ciruits are easy. How about long ones?*, in press
M. Geiger, M. Kagan, and E. Seber, *Resonance in long LC-ladder circuits*, in progress
M. Kagan and B. Mata, *Resistance distance in graphs with rotational symmetry*, in progress

Some new computer-aided models for the exceptional Zara graph on 126 vertices

Mikhail Klin[1,2] (Jointly with Leif Jørgensen and Matan Ziv-Av)

[1] *Ben-Gurion University of the Negev, Beer Sheva, Israel. klin@cs.bgu.ac.il*
[2] *Matej Bel University, Banska Bystrica, Slovakia.*

The exceptional Zara graph Z has the following properties:

- it is regular connected undirected graph on 126 vertices of valency 45;
- it contains a maximal clique C of size 6;
- each vertex x outside of clique C is adjacent to the same number $e_c = 2$ of neighbours in C.

The number e_c is called the *nexus* of C. (In fact all maximal cliques of Z have the same size 6 and nexus equal to 2.)

It was proved in [1] that these properties define unique, up to isomorphism, graph, namely the strongly regular graph Z with the parameters (126,45,80,12,18). The automorphism group $G = Aut(Z)$ is a rank 3 group of order 13063680.

Our interest to the graph Z stems from the investigation of so-called total graph coherent configurations. Namely, it was proved in [5] that an SRG Γ_1 with the same parameters and order of group appears as a suitable merging of the total graph coherent configuration, defined by the triangular graph $T(7)$. On this way we get a new model Γ_1 of Z, which is invariant with respect to S_7, having orbits of length 21 and 105 on vertices and 6 orbits on edges. This was established via the use of computer package COCO [2]. It is known that the graph Z has exactly 567 maximal cliques. For the created model Γ_1 these cliques split into three orbits of lengths 105, 210, 252; the members of each orbit have a nice combinatorial interpretation in terms of considered action of S_7.

The group $G = Aut(Z)$ contains as a subgroup of index 4 simple group $PSU(4,9)$ aka $U_4(3)$. This simple group is isomorphic to $P\Omega^-(6,3)$. Exactly this latter group was investigated by W.L. Edge in [3], where its primitive actions of degree 126 and 567 were clearly explained in classical terms of finite geometries.

In our attempts to create a reasonably clear model of Z, starting from a relatively small subgroup of G, acting transitively on the point set of Z, our attention was attracted to two conjugacy classes of subgroups of $U_4(3)$, both isomorphic to $PSU(3,3)$ of order 6048. In fact, for each of these two classes an overgroup $H = P\Gamma U(3,3)$ of order 12096 is also a subgroup of G.

First, the group H was regarded as the group $Aut(H(3))$ of the automorphisms of the classical hermitian unital with 28 points and 63 blocks of size 4. This unital $H(3)$ has exactly one orbit of spreads of length 63. Some properties of these spreads, that is partitions of the vertex set into 7 blocks, were carefully investigated. Using GAP [4], two conjugacy classes of subgroups L_1 and L_2 of H of order 96, both having orbits of length 4 and 24 on the points of $H(3)$, were detected and interpreted in ad hoc combinatorial terms. Transitive actions of H of degree 126 on cosets of L_1 and L_2 have rank 6 and 8 respectively. In each of the appearing association schemes there exists a rank 3 merging, with basic graphs Γ_2 and Γ_3, both isomorphic to Z.

Finally, a suitable amalgam of groups S_7 and H in G is investigated. It allows to outline a computer free proof of the fact that all the three graphs Γ_i, $i = 1,2,3$, are isomorphic to Z.

References

[1] A. Blokhuis, and A. E. Brouwer. *Uniqueness of a Zara graph on 126 points and non-existence of a completely regular two-graph on 288 points.* In J. de Graaf P.J. de Doelder and J.H. van Lint, editors, Papers dedicated to J.J. Seidel, EUT Report 84-WSK-03. EUT, august 1984.

[2] I. A. Faradžev and M. H. Klin. *Computer package for computations with coherent configurations*, Proc. ISSAC-91, pp. 219–223, Bonn, 1991. ACM Press.

[3] W. L. Edge. *The partitioning of an orthogonal group in six variables*, Proc. Roy. Soc. London. Ser. A 247 1958 539–549.

[4] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.8.7*; 2017, (`http://www.gap-system.org`).

[5] Matan Ziv-Av. *Computer aided investigation of total graph coherent configurations for two infinite families of classical strongly regular graphs*, Algorithmic algebraic combinatorics and Gröbner bases, 297–311, Springer, Berlin, 2009.

Automorphism groups of classical amorphic association schemes of Latin type

N. Kriger[1], A. Woldar[2]

[1] *Achva Academic College, nkriger1966@gmail.com*
[2] *Villanova University, USA, andrew.woldar@villanova.edu*

An association scheme is said to be **amorphic** if every possible merging of its classes yields an association scheme. We base our investigation on the family of **classical amorphic** association schemes of order p^2, p an odd prime, and automorphism group $H = \left(\mathbb{Z}_p^2\right) \rtimes \mathbb{Z}_p^*$. By definition, such schemes are mergings of the **complete classical affine** association scheme $\mathscr{A}_p$ of order p^2 and rank $p+2$, as introduced in [2] (see also [5]). Notably, there exists a bijection between classical amorphic schemes and partitions of the point set of the projective line $\mathrm{PG}(1,p)$ of cardinality $p+1$. To each such partition π with s classes of respective cardinalities i_j, $1 \le j \le s$, there corresponds an amorphic scheme $\mathscr{M}(\pi)$ of rank $s+1$ whose basis graphs have valency $(p-1)i_j,\ 1 \le j \le s$. Moreover, the automorphism group $Aut(\mathscr{M}(\pi))$ contains $H \rtimes S$ where S the stabilizer of π in the group $PGL(2,p)$. Note that here π is regarded as an ordered partition. As a consequence we obtain a proof of the following nice folklore result:

Proposition 1.1 *Amorphic scheme $\mathscr{M}(\pi)$ is Schurian if and only if S acts transitively on each class of π.*

An amorphic association scheme is said to be of **Latin type** if each class of its corresponding partition has size of at least 3. In other words, each basis graph of the scheme has valency at least $l(p-1),\ l \ge 3$ and this naturally corresponds to a set of $l-2$ pairwise orthogonal Latin squares.

Extending investigations in [6], the author NK arranged a new round of computer experimentation aimed at classifying, up to isomorphism, all classical amorphic schemes of Latin type for primes $p \in \{5,7,11,13\}$. Schemes were summarily generated, checked to see if Schurian, and their automorphism groups determined. Full results were obtained for $p = 5,7,11$, and partial results for $p = 13$ (due to limited computer memory). The number of considered schemes is indicated below.

prime p	5	7	11	13
number of schemes	1	4	526	3251

More detailed information about these schemes will be presented in our talk, especially with regard to the following curious observation.

Proposition 1.2 *For all considered values of p and ordered partitions π, one has*

$$Aut(\mathscr{M}(\pi)) \cong H \rtimes S$$

In other words, all automorphisms of association schemes of Latin type are of geometric nature.

In our talk, we shall also discuss recent theoretical activity aimed at extending Proposition 1.2 to all primes p. A promising pathway is suggested, namely the amalgamation of two diverse methodologies: classical results on transitive permutation groups of prime-square order on one hand (e.g., see [1, 4, 7]) and symmetries of nets and Desarguesian planes of order p on the other hand (e.g., see the discussion in [3]).

Acknowledgment. Special thanks are due to Misha Klin for helpful intermediation between the two authors. We are also grateful to Matan Ziv-Av for creating a few helpful GAP routines used in the course of computer experimentation.

References

[1] E. Dobson and D. Witte, *Transitive permutation groups of prime-squared degree*. J. Algebraic Combin. **16**, 1, pp. 43-69 (2002).

[2] Ja. Ju. Gol'fand, A. V. Ivanov, M. H. Klin, *Amorphic cellular rings*, in: I.A. Faradžev, et al. (eds), *Investigations in Algebraic Theory of Combinatorial Objects*, Kluwer Academic Publishers, Dordrecht, pp. 167–186 (1994). (Translation from the Russian original: Investigations in Algebraic Theory of Combinatorial Objects (Moscow, VNIISI, 1985) 32-38 and 39-49.)

[3] A. Heinze and M. H. Klin, *Loops, Latin squares and strongly regular graphs: An algorithmic approach via Algebraic Combinatorics*, in: M. Klin et al, Algorithmic Algebraic Combinatorics and Gröbner Bases, Springer-Verlag Berlin Heidelberg, pp. 3-65 (2009).

[4] G. A. Jones and K. D. Soomro, *On a theorem of Wielandt concerning simply primitive groups*. Math. Proc. Cambridge Philos. Soc. **92**, 3, pp. 419-423 (1982).

[5] M. H. Klin, N. Kriger, A. Woldar, *On the existence of self-complementary and non-self-complementary strongly regular graphs with Paley parameters.* J. Geom. **107** , 2, pp. 329-356 (2016).

[6] N. Kriger, *Investigation of Strongly Regular Graphs of Latin Square Type and Related Combinatorial Objects*, Ben-Gurion University of the Negev, PhD dissertation, (2014).

[7] H. Wielandt, *Permutation groups through invariant relations and invariant functions*, Lecture Notes, The Ohio State Univ., Columbus, OH, (1969).

Enumeration of actions of cyclic groups on compact closed surfaces

R. Nedela[1]

[1]*New Technologies for Information Society, University of West Bohemia, Pilsen, Czech Republic, nedela@savbb.sk*

Between discrete actions of groups on surfaces, the actions of cyclic groups play a central role. They appear naturally as coefficients in enumeration formulae for coverings between manifolds, for maps and hypermaps with given number of edges and in many other problems. Therefore, we need to count the number of them up to an equivalence relation given by the conjugacy of the kernels of the natural epimorphisms from the associated orbifold fundamental groups. For surfaces of small genera g, the size of the cyclic group is bounded by a linear function of g. For small genera one can solve the problem by the standard procedure enumerating low index subgroups in a group given by a presentation. The respective commands are implemented in MAGMA or in GAP. In the particular case of cyclic groups, Harvey (1966) derived a criterion for an existence of a cyclic action on a surface of genus g determining an orbifold with a prescribed signature. In a paper with A. Mednykh (2006) we have derived a multivariable multiplicative function determining the number of cyclic actions on a surface of genus g of a prescribed signature. The function was determined in an additive form.

Later, V. Liskovets derived an equivalent multiplicative expression of the function. This simplifies the computations significantly, and as a result, we are able to classify the cyclic actions for surfaces of genera up to 300. The tables determining the numbers of cyclic actions were done with the help of the software packages MAGMA and MATHEMATICA.

Algebraic Graph Theory Algorithms For Modern Computer Architectures

S. Reichard[1]

[1] *Institut für Algebra, Technische Universität Dresden, Germany, sven.reichard@tu-dresden.de*

Algorithms play a big role in AGT. Examples of tasks that are solved algorithmically include the following:

- Isomorphism tests of coherent configurations;
- Finding the full automorphism group of a coherent configuration;
- Stabilization procedures such as Weisfeiler-Lehman, which finds the smallest coherent configuration containing a given set of relations;
- Enumeration of mergings of coherent configurations.

Whereas computers used to be modeled using a single central processing unit having access to a uniform random access memory this description is no longer accurate.

Modern computers, even in the consumer PC range, provide parallelism on several levels. Wide registers can accomodate lots of data and the possibility of SIMD processing (Single instruction, multiple data). Processors contain several more or less independent processing units or cores. Moreover, single cores can execute interleave several threads of instruction, leading to apparent parallel execution (SMT, simultaneous multithreading). Computers appear which contain several processors, and finally, large numbers of computers are interconnected in networks.

Since each of the processors has its own memory the assumption of uniform memory the assumption of uniform memory access is not fulfilled either. But even on a single processor we deal with the fact that faster memory is more expensive than slower memory. This leads to a hierarchical organization of memory, with six or more levels of slower and more abundant memory, ranging from hundreds of bytes of registers over caches and DRAM to terabytes on a hard drive.

Since memory access dominates arithmetical computations in many problems in AGT, the layout of data in memory is crucial for high performant algorithms.

We look at implementations of two algorithms:

The algorithm for finding coherent configurations by Weisfeiler-Lehman [3] was originally stated in terms of matrices:

1. Replace entries of the given matrix with non-commuting indeterminates

2. Compute the square of the matrix

3. Repeat until the number of distinct entries is stable.

Two implementations have been described [1], with different practical and theoretical complexity properties. We give a new implementation which is practically faster on many examples and has moderate space requirements.

S-rings are particular instances of association schemes. They are invariant under a regular permutation group. S-rings over a group H are thus mergings of the centralizer ring of a regular action of H. These correspond to certain partitions of H.

Ziv-Av has enumerated all S-rings over groups of order up to 63 [4]. The elementary abelian group of order 64 was previously dealt with by the author.

The enumeration of mergings proceeds in two stages:

1. Enumeration of "good" subsets of H.

2. Constructing adequate partitions from those sets.

For most groups the first stage is the hardest part. Here we need to consider all subsets of H, so the search space has the shape of a hypercube. We consider the following optimizations:

- Using the automorphism group to reduce the search tree.
- Coarse parallelism, processing different parts of the tree simultaneously.
- Using the self-similarity of the search space. By reordering the search we can make use of SIMD instructions.

References

[1] L. Babel, I.V Chuvaeva, M. Klin, and D.V Pasechnik. Algebraic combinatorics in mathematical chemistry. Methods and algorithms. II. Program implementation of the Weisfeiler-Leman algorithm. https://arxiv.org/abs/1002.1921v1, 1997.

[2] Barbara Chapman, Gabriele Jost, and Ruud van der Paas. *Using OpenMP: Portable Shared Memory Parallel Programming*. Scientific and Engineering Computation. The MIT Press, 2007.

[3] Boris Weisfeiler. *On Construction and Identification of Graphs*. Springer Berlin Heidelberg, Berlin, Heidelberg, 1976.

[4] Matan Ziv-Av. Enumeration of Schur rings over small groups. In Vladimir P. Gerdt, Wolfram Koepf, Werner M. Seiler, and Evgenii V. Vorozhtsov, editors, *Computer Algebra in Scientific Computing: 16th International Workshop, CASC 2014, Warsaw, Poland, September 8-12, 2014. Proceedings*, pages 491–500. Springer International Publishing, Cham, 2014.

The Clebsch graph on the crossroads of Algebraic Geometry and Algebraic Graph Theory

M. Klin[1], E. Shamovich[2]

[1] *Ben-Gurion University of the Negev, Beer-Sheva, Israel {klin}@math.bgu.ac.il*
[2] *Technion - Israel Institute of Technology, Haifa, Israel shamovich@techunix.technion.ac.il*

The Clebsch graph Cl is a strongly regular graph (SRG) with the parameters (16,5,10,0,2)S and primitive rank 3 automorphism group of order 1920, isomorphic to the spilt extension $E_{16} : S_5$. It is one of the six known primitive triangle free SRGs with 5,10,16,56,77 and 100 vertices. All these graphs appear as (induced) subgraph of the graph $NL_2(10)$ with 100 vertices, discovered by Dale Mesner in 1956 and also known as the Higman-Sims graph, see [6] for details. The question about the existence of other primitive triangle-free SRGs remains open for a long while and seems to be one of the most challenging problems in AGT.

The name Clebsch graph was coined by J.J. Seidel in [8], sometimes this name is attributed to the complementary to Cl graph of valency 10. Many nice models of Cl appear on the home page of Andries Brouwer [1].

Being originally educated in classical geometry of XIXth century, Seidel was referring to the paper [2]. While the name itself was commonly used for about half a century, it seems that its roots were not discussed properly in literature.

According to procedure, described by A. Rudvalis [7], starting from Cl, one gets a symmetric design on 16 vertices, usually called biplane. All biplanes on 16 points are well-known, see e.g. [5]. The one, which appears from Cl is sometimes called the nicest biplane B_6 (on 16 points). According to the procedure by Rudvalis, which involves polarities of designs, the graph Cl is reconstrutable from B_6.

A remarkable issue is that some of the objects equivalent to biplanes on 16 points were also discoverdd in AG, in the framework of Kummer surfaces, see [4]. The new incaranation of the classical results by Hudson in modern clothes of AG appears in [3]. In this talk we are trying to tie all these loose ends, using in particular facilites of computer packages.

In fact, Clebsch studied in his classical paper [2] a class of quartic surfaces in $\mathbf{P}^3$ obtained as the image of four generic cubic homogeneous polynomials in three variables, that vanish at a given set of of five points in generic position in $\mathbf{P}^2$. In modern terms we can construct the surface by looking at the blowup of $\mathbf{P}^2$ in five points in general position. The blowup surface is smooth and can be embedded in $\mathbf{P}^4$. This is a Del Pezzo surface of degree 4 in $\mathbf{P}^4$ and projecting this surface from a generic point not on the surface, we obtain the Clebsch quartic in $\mathbf{P}^3$. The surface has 16 lines on it obtained as the images of the exceptional divisor, the

line connecting two points in the blowup set and the unique conic passing through all of the five points. These are the vertices of the classical copy of *Cl* and the edges connect intersecting pairs of lines. We use Macaulay2 to construct *Cl* using the original Clebsch surface and the routine for constructing the Fano scheme of lines on the surface. An interesting connection, highlighted by Sturmfels and his collaborators, is that the Clebsch graph appears also via tropicalization of a degree four Dnl Pezzo surface, namely the tropicalization is a cone over the Clebsch graph.

One can also consider a Kummer surface, namely a singular quartic in $\mathbf{P}^3$ that has only nodes as singularities and a maximal number of them (sixteen in this case). A Kummer surface gives naturally a rise to a biplane via considering the sixteen nodes and the sixteen curves passing each through exactly six of those nodes. As mentioned above, one can obtain *Cl* from the configuration by the use of polarities.

A main question is can one obtain *Cl* from a Kummer surface using only the algebro-geometric toolkit? It was shown by Skorobogatov in [9], that every Del Pezzo surface of degree 4 admits a degree 2 branched covering map from the desingularization of a Kummer surface, that sends lines on the desingularization to the 16 lines on our Del Pezzo surface. It is now natural to ask whether this gives a geometric picture of the above stated classical combinatorial fact? Thus finally we report about our computer aided efforts to clarify this issue.

Acknowledgements.

We thank Yue Ren, Bernd Sturmfels and Ilya Tyomkin for helpful communication.

References

[1] Home page of Andries Brouwer, *http://www.win.tue.nl/ aeb/*

[2] A. Clebsch, *Ueber die Flächen vierter Ordnung, welche eine Doppelcurve zweiten Grades besitzen*, J. Reine Angew. Math.,69, (1868), 142–184 pp.

[3] M. R. Gonzalez-Dorrego, $(16,6)$ *configurations and geometry of Kummer surfaces in* $\mathbf{P}^3$, Mem. Amer. Math. Soc. 107 (1994), no. 512, vi+101 pp.

[4] R. W. H. T. Hudson, "Kummer's quartic surface", Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1990.

[5] D. R. Hughes and F. C. Piper, "Design theory". Second edition. Cambridge University Press, Cambridge, 1988.

[6] M. H. Klin and A. J. Woldar, *Dale Mesner, Higman & Sims, and the strongly regular graph with parameters* $(100,22,0,6)$, Bull. Inst. Combin. Appl. 63 (2011), 13–35 pp.

[7] A. Rudvalis (v,k,λ)*-graphs and polarities of* (v,k,λ)*-designs*, Mathematische Zeitschrift 120 (1971), 224–230 pp.

[8] J. J. Seidel, *Strongly regular graphs with* $(-1,1,0)$ *adjacency matrix having eigenvalue* 3, Linear Algebra and Appl. 1 (1968), 281–298 pp.

[9] A. Skorobogatov, *del Pezzo surfaces of degree 4 and their relation to Kummer surfaces*, Enseign. Math. (2) 56 (2010), 73–85 pp.

Constructive enumeration of the coherent configurations

M. Ziv-Av[1]

[1] *Ben-Gurion University of the Negev, Beer-Sheva, Israel. matan@svgalib.org*

A coherent configuration is a partition of the arc set of a complete directed graph with some extra requirements [1]. Coherent configurations correspond to (some) subalgebras of the complete matrix algebra of the corresponding order. As such a two faced concept, coherent configurations play a significant role in algebraic graph theory.

Using a computer we constructed all coherent configurations of orders no more than 15 (up to isomorphism). One result of this enumeration is discovery of (the unique) non-Schurian coherent configuration of order 14 [2]. All coherent configurations of orders up to 13 are Schurian, so this is the smallest non-Schurian coherent configuration.

We will consider this project in a wider context by discussing computer aided enumeration efforts for some subclasses of coherent configurations such as association schemes, Schur rings, and strongly regular graphs.

The talk will also include a description of the techniques used to achieve the reported results.

References

[1] E. Bannai and T. Ito. *Algebraic combinatorics. I. Association schemes*, The Benjamin/Cummings Publishing Co., Inc., Menlo Park, CA, (1984).

[2] M. Klin and M. Ziv-Av *A non-Schurian coherent configuration on 14 points exists*, M. Des. Codes Cryptogr. (2016). doi:10.1007/s10623-016-0258-8

Session 15

High-Performance Computer Algebra

Session chairs:

Jeremy Johnson
Drexel University, USA

Gennadi Malaschonok
Tambov State University, Russia

Marc Moreno Maza
Waterloo University, ON, Canada

Interactions between high-performance computing and computer algebra: overview and perspectives

Jeremy Johnson[1], Gennadi Malaschonok[2], Marc Moreno Maza[3]

[1] *Drexel University, Philadelphia PA, USA, jjohnson@cs.drexel.edu*
[2] *Tambov State University, Russia, malaschonok@gmail.com*
[3] *U. Western Ontario, London, Ontario, Canada, moreno@csd.uwo.ca*

This introductory talk is a (certainly subjective) presentation of the interactions between high-performance computing (HPC) and computer algebra. We shall start with an overview of passed achievements based, in particular, on the PASCO workshop series. Then, we shall discuss the many opportunities and challenges that modern computer hardware offer to computer algebraists. This latter part will also serve as a short tutorial for participants unfamiliar with fundamental HPC concepts and techniques.

Fast construction of a lexicographic Gröbner basis of the vanishing ideal of a set of points

X. Dahan[1]

[1] *Ochanomizu University, Japan, dahan.xavier@ocha.ac.jp, xdahan@gmail.com*

Problem Given a set V of Zariski-closed points lying in $\bar{k}^n$, $\bar{k}$ an algebraic closure of a base field of interest k, its *vanishing ideal* $I(V) \subset k[X_1,\ldots,X_n]$ is the radical, 0-dimensional ideal of polynomials vanishing on V. We are interested in constructing a minimal lexicographic Gröbner basis $\mathscr{G}$ of $I = I(V)$.

Result The main outcome is Result 1. below. In HPC, a complexity analysis often precedes an implementation, and a challenge is indeed that benchmarks meet the expected complexity bounds. This is where lies this work (A preliminary implementation is available in Maple, but cannot be qualified as HPC currently).

Notations Lex, LexGB stands for lexicographic and lexicographic Gröbner basis respectively. Given a set $E \subset k[X_1,\ldots,X_n]$, then $E_{\leq \ell}$ denotes the set $E \cap k[X_1,\ldots,X_\ell]$.

1. There is a minimal lexicographic Gröbner basis $\mathscr{G}$ whose any of its polynomial can be computed in $O(\mathsf{A}(D_1) + \mathsf{A}(D_2) + \cdots + \mathsf{A}(D_n))$ arithmetic operations where $D_i = |V_{\leq i}| = \dim_k(k[X_1,\ldots,X_i]/I_{\leq i})$, and $\mathsf{A}(d)$ is the number of arithmetic operations over k necessary to build Lagrange idempotents of d points by using sub-product tree techniques ($\mathsf{A}(d) = \mathsf{M}(d)\log(d)$. Using Schönhage-Strassen fast multiplication one has $\mathsf{M}(d) = O(d\log(d)\log\log(d))$, or $\mathsf{M}(d) = d^2$ using naive polynomial multiplication).
2. the polynomials in $\mathscr{G}$ present a special structure, sort of redundant factors that allows to recycle already computed polynomials and Lagrange cofactors (and those computed in the sub-product trees) to considerably lower the number of arithmetic operations to compute new polynomials in $\mathscr{G}$.
3. Any polynomial in $\mathscr{G}$, say w.l.o.g. in $k[X_1,\ldots,X_n] \setminus k[X_1,\ldots,X_{n-1}]$, verifies a generalization of Gianni-Kalkbrener theorem: if $\alpha \in V_{\leq \ell}$ is such that $\deg_{X_{\ell+1}}(g(\alpha, X_{\ell+1},\ldots,X_n)) < \deg_{X_{\ell+1}}(g)$, then $g(\alpha, X_{\ell+1},\ldots,X_n) = 0$.
4. $\mathscr{G}$ is not the reduced Gröbner basis in general, hence has more coefficients, but its coefficients are smaller.
5. to V, we first build its *decomposition points tree* $\mathscr{T}(V)$. The *arithmetic* complexity for solving "Problem" depends only of the shape of this tree (of course

not the case for the bit complexity where the bit-size of the input points matters also).

Brief overview of previous works The above results are related to a number of previous works. We only refer to the most relevant ones that put into perspective the above statements. The numbering below refers to that of above.

1. Lederer [10] who has produced the most accomplished interpolation formulas focuses on the *reduced* Gröbner basis, which complicates his task quite considerably. This leaves a sharp complexity analysis quite difficult — indeed there is none; this stems for the fact that many additional polynomials must be computed on demand to cancel too large monomials. The reduced lexGB has a less satisfactory specialization property (see [1, 8]).

Before it was understood that the configuration of points in V could give the set of standard monomials for the lexicographic oder (Cf. [3, 13, 6, 5]), algorithms based on linear algebra were predominant. They give roughly an $O(nD^3)$ [2, 14] arithmetic cost (but are *not* constrained to the lex order).

A related problem concerns the computation of a separating basis of the vector space $k[X_1,\ldots,X_n]/I$. By "separating" we mean polynomials $\{p_v\}_{v\in V}$ such that $p_v(w)=\delta_{vw}$ (Kronecker symbol). Such a basis is closely related to multivariate Lagrange bases: Lundqvist [12] claims a cost of $O(D^2)$ points, but using fast interpolation it can be reduced to a complexity similar to that stated in Result 1. above. As for Hermite interpolation, in [11] linear algebra exploits the possibly very low displacement rank of the interpolating matrix to propose $O((\tau+3)D^2)$ (for Vandermonde we have $\tau=2$ hence of the same order of Lagrange interpolation with naive multiplication).

2. Starting with Lazard's structural theorem ([9], lexGB in two variables), several authors have shown that a somewhat comparable result holds for more than two variables (to cite a few [13], and implicitly in [5, 10, 6]), at least in the radical 0-dimensional case. However, few, if none, considered the relationship between factors of two different polynomials in $\mathscr{G}$. This is a key point to recycle computations and to dramatically decrease the complexity, even if it is not easy to quantify.

3. The stability of Gröbner bases under specialization refers to the fact that a specialized Gröbner basis remains a Gröbner basis of the specialized ideal. Beyond the seminal Gianni-Kalkbrener result [7], Becker [1] then Kalkbrener [8] showed that whenever a degree decrease occurs after specialization, then the polynomial reduces to zero modulo the other polynomials. As stated, the specific Gröbner basis that we construct verifies a stronger property: no degree decrease, or else it specializes to zero, as in Gianni-Kalkbrener's theorem.

4. The maximal bit-size among all coefficients of polynomials appearing in $\mathscr{G}$ can be estimated to be *roughly* in $O(nD^2h^2)$ where h is the maximal bit-size of the components of input points. This strategy follows that of [4]. Again, obtaining such a sharp result for the reduced lexGB is not easy.

5. this is interesting if we see the formula constructing the basis $\mathscr{G}$ as an algebraic circuit that computes the polynomials in $\mathscr{G}$. This circuit depends only of the shape of the tree.

Implementation We have implemented *naively* the interpolation formula that computes $\mathscr{G}$ in Maple and will show experimental results that illustrate all the points mentioned above.

References

[1] T. Becker. Gröbner bases versus D-Gröbner bases, and Gröbner bases under specialization. *Applicable Algebra in Engineering , Communications and Computing*, 5:1–8, 1994.

[2] B. Buchberger and H. Möller. The construction of multivariate polynomials with preassigned zeros. In *Lecture Notes in Computer Science (EUROCAM'82)*, volume 144, pages 24–31, London, UK, 1982.

[3] L. Cerlienco and M. Mureddu. From algebraic sets to monomial linear bases by means of combinatorial algorithms. *Discrete Mathematics*, 139(1-3):73–87, 1995.

[4] X. Dahan and É. Schost. Sharp estimates for triangular sets. In *ISSAC '04: Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, pages 103–110. ACM Press, 2004.

[5] B. Felszeghy, B. Ráth, and L. Rónyai. The lex game and some applications. *J. of Symbolic Comput.*, 41(6):663 – 681, 2006.

[6] S. Gao, V. Rodrigues, and J. Stroomer. Gröbner basis structure of finite sets of points. http://www.math.clemson.edu/~sgao/pub.html, 2003. Preprint (16 pages).

[7] P. Gianni. Properties of Gröbner bases under specialization. In J.H. Davenport, editor, *In Proc. of EUROCAL'87*, Lecture Notes in Computer Science (378), pages 293–297. Springer, Berlin, 1987.

[8] M. Kalkbrener. On the stability of Gröbner bases under specialization. *J. Symbolic Comput.*, 24(2):51–58, 1997.

[9] D. Lazard. Ideal bases and primary decomposition: case of two variables. *J. Symbolic Comput.*, 1(3):261–270, 1985.

[10] M. Lederer. The vanishing ideal of a finite set of closed points in affine space. *J. of Pure and Applied Algebra*, 212:1116–1133, 2008.

[11] Na Lei, Yuan Teng, and Yu-xue Ren. A fast algorithm for multivariate hermite interpolation. *Applied Mathematics-A Journal of Chinese Universities*, 4(29):438–454, 2014.

[12] Samuel Lundqvist. Vector space bases associated to vanishing ideals of points. *Journal of Pure and Applied Algebra*, 214(4):309 – 321, 2010.

[13] M. G. Marinari and T. Mora. A remark on a remark by Macaulay or enhancing Lazard structural theorem. *Bull. Iranian Math. Soc.*, 29(1):1–45, 85, 2003.

[14] M.G. Marinari, H. M. Moeller, and T. Mora. Gröbner bases of ideals defined by functionals with an application to ideals of projective points. *Applicable Algebra in Engineering, Communication and Computing*, 4(2):103–145, 1993.

A Parallel Compensated Horner Scheme

S. Graillat[1], Y. Ibrahimy, C. Jeangoudoux[1], C. Lauter[1]

[1] *Sorbonne Universités, UPMC Univ Paris 06, CNRS, LIP6 UMR 7606, F-75005, Paris, France*
{stef.graillat,clothilde.jeangoudoux,christoph.lauter}@lip6.fr

The Compensated Horner Scheme [1, 2] is an accurate and fast algorithm to evaluate univariate polynomials in floating-point arithmetic. The accuracy of the computed result is similar to the one given by the Horner scheme computed in twice the working precision. The implementation of the Compensated Horner Scheme runs at least as fast as existing implementations of Horner Scheme producing the same output accuracy.

It is based on the so-called *error-free transformations*. These are algorithms that make it possible to compute (in pure floating-point arithmetic) the rounding error for the elementary operations (addition, subtraction and multiplication). Indeed, it is possible to show that these elementary rounding errors can be represented exactly as floating-point numbers (unless underflow or overflow occurs).

Parallelizing compensated algorithms is tedious even for summation and dot product algorithms [3]. In this talk, we will present a parallel version of the Compensated Horner Scheme. Some experiments on multicore and Graphics Processor Units (GPU) architectures will be presented to show the efficiency of this algorithm.

References

[1] S. Graillat, N. Louvet, and Ph. Langlois. Compensated Horner scheme. Research Report 04, Équipe de recherche DALI, Laboratoire LP2A, Université de Perpignan Via Domitia, France, 52 avenue Paul Alduy, 66860 Perpignan cedex, France, July 2005.

[2] S. Graillat, Ph. Langlois, and N. Louvet. Algorithms for accurate, validated and fast polynomial evaluation. *Japan J. Indust. Appl. Math.*, 26(2-3):191–214, 2009.

[3] N. Yamanaka, T. Ogita, S. M. Rump, and S. Oishi. A parallel algorithm for accurate dot product. *Parallel Comput.*, 34(6-8):392–410, 2008.

Exhaustive search of optimal formulae for bilinear maps

S. Covanov[1]

[1] *Université de Lorraine, France, {svyatoslav.covanov}@inria.fr*

Finding optimal formulae for computing bilinear maps is a problem of algebraic complexity theory [3, 2, 16, 8], initiated by the discoveries of Strassen [16] and Karatsuba [9]. It consists to determine almost optimal algorithms for important problems of complexity theory, among which the well studied complexity of matrix multiplication [16, 5, 10] and the complexity of polynomial multiplication [9, 17, 15, 6].

In the field of complexity of polynomial multiplication, the first improvement over the schoolbook method came from Karatsuba [9] in 1962, who proposed a decomposition of the bilinear map corresponding to the product of two polynomials of degree 2

$$P = p_0 + p_1 X \text{ and } Q = q_0 + q_1 X. \tag{1}$$

The product $P \cdot Q$ requires, to be computed, 4 multiplications using the schoolbook algorithm: p_0q_0, p_1q_0, p_0q_1, p_1q_1. With the Karatsuba algorithm, the coefficients of the product $P \cdot Q$ can be retrieved from the computation of the 3 following multiplications: p_0q_0, $(p_0+p_1)(q_0+q_1)$, p_1q_1. In particular, Karatsuba's algorithm can be used to improve the binary complexity of the multiplication of two n-bit integers: instead of $O(n^2)$ with the naive schoolbook algorithm, we obtain $O(n^{\log_2 3})$. Then, given a degree $d > 1$, computing the minimal amount of multiplications required for the product of polynomials of degree d leads to even better complexities and produces optimal formulae for a particular product.

The main obstacle to finding optimal formulae is the fact that the decomposition of bilinear maps is known to be NP-hard [7]. Montgomery proposed in [11] an algorithm to compute such a decomposition for the particular case of polynomials of small degree over a finite field. The author takes advantage of the fact that the number of all optimal formulae is limited on a finite field. He gets new formulae for the multiplication of polynomials of degree 5, 6 and 7 over $\mathbb{F}_2$. In [12], Oseledets proposes a heuristic approach and uses the formalism of vector spaces to solve the bilinear rank problem for the polynomial product over $\mathbb{F}_2$. Later, Barbulescu et al. proposed in [1] a unified framework, developping the idea proposed by Oseledets using the vector

spaces formalism, permitting the authors to compute the bilinear rank of different applications, such as the short product or the middle product over a finite field. Their algorithm allows one to generate all the possible rank decomposition of any bilinear map over a finite field. This work is the main inspiration of the current presentation.

Our work is an improvement to the algorithm introduced in [1], allowing one to increase the family of bilinear maps over a finite field for which we are able to compute all the optimal formulae. Our algorithm relies on the automorphism group stabilizing a bilinear map, seen as a vector space, and on a topological invariant of such a vector space. It can be used for proving lower bounds on the rank of a bilinear map and it has applications for improving upper bounds on the Chudnovsky-Chudnovsky algorithms [4, 14, 13]. Especially, we compute all the decompositions for the short product of polynomials P and Q modulo X^5 and the product of 3×2 by 2×3 matrices. The latter problem was out of reach with the method used in [1]: we prove, in particular, that the set of possible decompositions for this matrix product is essentially unique, up to the automorphism group.

References

[1] R. Barbulescu, J. Detrey, N. Estibals, and P. Zimmermann. *Arithmetic of finite fields: 4th International Workshop, WAIFI 2012, Bochum, Germany, July 16-19, 2012. Proceedings*, chapter Finding Optimal Formulae for Bilinear Maps, pages 168–186. Springer, 2012. doi:10.1007/978-3-642-31662-3_12.

[2] R. W. Brockett and D. Dobkin. On the optimal evaluation of a set of bilinear forms. *Linear Algebra and its Applications*, 19(3):207 – 235, 1978. doi:10.1016/0024-3795(78)90012-5.

[3] P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic Complexity Theory*. Springer, 1st edition, 2010.

[4] D. Chudnovsky and G. Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Journal of Complexity*, 4(4):285 – 316, 1988. doi:10.1016/0885-064X(88)90012-X.

[5] D. Coppersmith and S. Winograd. Computational algebraic complexity editorial matrix multiplication via arithmetic progressions. *Journal of Symbolic Computation*, 9(3):251 – 280, 1990. doi:10.1016/S0747-7171(08)80013-2.

[6] D. Harvey, J. van der Hoeven, and G. Lecerf. Even faster integer multiplication. Technical report, ArXiv, 2014. arXiv:1407.3360.

[7] J. Håstad. Tensor rank is np-complete. *Journal of Algorithms*, 11(4):644 – 654, 1990. doi:10.1016/0196-6774(90)90014-6.

[8] J. JáJá. Optimal evaluation of pairs of bilinear forms. *SIAM Journal on Computing*, 8(3):443–462, 1979. doi:10.1137/0208037.

[9] A. Karatsuba and Y. Ofman. Multiplication of multidigit numbers on automata. *Soviet Physics-Doklady*, 7:595–596, 1963. (English translation).

[10] F. Le Gall. Powers of tensors and fast matrix multiplication. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ISSAC '14, pages 296–303. ACM, 2014. doi:10.1145/2608628.2608664.

[11] P. Montgomery. Five, six, and seven-term Karatsuba-like formulae. *Computers, IEEE Transactions on*, 54(3):362–369, 2005. doi:10.1109/TC.2005.49.

[12] I. Oseledets. Optimal Karatsuba-like formulae for certain bilinear forms in gf(2). *Linear Algebra and its Applications*, 429(8-9):2052 – 2066, 2008. doi:10.1016/j.laa.2008.06.004.

[13] M. Rambaud. *Arithmetic of Finite Fields: 5th International Workshop, WAIFI 2014, Gebze, Turkey, September 27-28, 2014. Revised Selected Papers*, chapter Finding optimal Chudnovsky-Chudnovsky multiplication algorithms, pages 45–60. Springer, 2015. doi:10.1007/978-3-319-16277-5_3.

[14] H. Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. *Journal of Complexity*, 28(4):489 – 517, 2012. doi:10.1016/j.jco.2012.02.005.

[15] A. Schönhage and V. Strassen. Schnelle multiplikation großer zahlen. *Computing*, 7(3-4):281–292, 1971. doi:10.1007/BF02242355.

[16] V. Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13(4):354–356. doi:10.1007/BF02165411.

[17] A. L. Toom. The complexity of a scheme of functional elements realizing the multiplication of integers. *Soviet Mathematics Doklady*, 3:714–716, 1963. (English translation).

Minimizing arithmetic and communication costs for faster matrix computations

Oded Schwartz[1]

[1] *School of Computer Science and Engineering, The Hebrew University of Jerusalem, Israel*
odedsc@cs.huji.ac.il

Algorithms are often evaluated in terms of the number of arithmetic operations they performed. However, on today's machines, communication, i.e., moving data through memory hierarchies and among processors often requires much more time (and energy) than performing computations. Hardware trends suggest that the relative costs of such communication will only increase. In this talk I will review several recent algorithms for reducing both arithmetic and communication costs, and show matching lower bounds, proving them to be optimal.

Based on joint papers with Grey Ballard, James Demmel, Andrew Gearhart, Olga Holtz, Elaye Karstadt, Ben Lipshitz, Yishai Oltchik, and Sivan Toledo.

Communication-efficient parallel Bruhat decomposition

Alexander Tiskin[1]

[1] *University of Warwick, Coventry, UK, A.Tiskin@warwick.ac.uk*

We consider the problem of computing the Bruhat decomposition of a matrix on a parallel computer with p processors. The communication and synchronisation between processors are accounted for according to Valiant's bulk-synchronous parallel (BSP) computation model [**?**, **?**, **?**]. Our algorithm obtains the Bruhat decomposition of an $n \times n$ matrix in local computation $O(n^3/p)$ per processor, communication $O(n^2/p^\alpha)$ per processor, and $O(p^\alpha)$ barrier synchronisations, for an arbitrary α, $1/2 \leq \alpha \leq 2/3$. The algorithm generalises the previously known approaches to generic and generic pairwise Gaussian elimination [**?**, **?**], and matches the communication lower bound $\Omega(n^2/p^{2/3})$ on parallel matrix multiplication [**?**].

References

[1] L. G. Valiant, A bridging model for parallel computation, Communications of the ACM 33 (8) (1990) 103–111.

[2] W. F. McColl, Scalable computing, in: J. van Leeuwen (Ed.), Computer Science Today: Recent Trends and Developments, Vol. 1000 of Lecture Notes in Computer Science, Springer-Verlag, 1995, pp. 46–61.

[3] A. Tiskin, Bulk-synchronous parallel Gaussian elimination, Journal of Mathematical Sciences 108 (6) (2002) 977–991.

[4] R. H. Bisseling, Parallel Scientific Computation: A structured approach using BSP and MPI, Oxford University Press, 2004.

[5] D. Irony, S. Toledo and A. Tiskin. Communication lower bounds for distributed-memory matrix multiplication. Journal of Parallel and Distributed Computing, 64, 9, pp. 1017–1026, 2004.

[6] A. Tiskin. Communication-efficient parallel generic pairwise elimination. Future Generation Computer Systems, 23, 2, pp. 179–188, 2007.

Efficient Algorithms for Evaluating High-Degree Matrix Polynomials

Niv Hoffman[1], Oded Schwartz[2], Sivan Toledo[1]

[1] *Blavatnik School of Computer Science, Tel-Aviv University, Israel,* stoledo@tau.ac.il

[2] *School of Computer Science and Engineering, The Hebrew University of Jerusalem, Israel*

In the early 1970s, Patterson and Stockmeyer discovered a surprising, elegant, and very efficient algorithm to evaluate a matrix polynomial. Later in the 1970s, Van Loan showed how to reduce the memory consumption of their algorithm, addressing an issue that was important back then. There has not been any significant progress in this area since, in spite of dramatic changes in computer architecture and in closely-related algorithmic problems.

We revisit the problem and apply to it both cache-miss reduction methods and new algorithmic tools. Our main contributions are:

- We develop a new block variant of Van-Loan's algorithm, which is usually almost as memory-efficient as Van-Loan's original variant, but much faster.
- We develop two algorithms that reduce the matrix to its Schur form, to speed up the computation relative to both Patterson and Stockmeyer's original algorithm and Van Loan's variants, including the new block variant. One algorithm exploits the fact that multiplying triangular matrices is faster (by up to a factor of 6) than multiplying dense square matrices. The other algorithm partitions the problem into a collection of smaller ones using a relatively recent algorithm due to Davies and Higham.
- We analyze the number of cache misses that the main variants generate, thereby addressing a major cost on modern architecture. The analysis is theoretical and it explains our experimental results, discussed below.
- We evaluate the performance of the direct algorithms (the ones that do not reduce the matrix to Schur form), both existing and new, pinpointing algorithms that are particularly effective.
- We predict the performance of algorithms that reduce the matrix to Schur form using an empirically-based performance model of the performance of their building blocks.

High-Performance Kernels for Exact Linear Algebra

Jeremy Johnson[1], Tze Meng Low[2], Matthew Lambert[3], Peter Oostema[2], B. D. Saunders[3]

[1] *Drexel University, Philadelphia PA, USA, jjohnson@cs.drexel.edu*
[2] *Carnegie Mellon University, Pittsburgh PA, USA, lowt,poostema@andrew.cmu.edu*
[3] *University of Delaware, Newark DE, USA, lambert,saunders@udel.edu*

High-performance linear algebra libraries are typically built on top of fast matrix-matrix multiplication kernels. Significant effort, by the numerical linear algebra community, has been devoted to the implementation and optimization of these kernels on a wide variety of computer architectures [1, 3, 4].

The computer algebra community has taken advantage of this work in [5], avoiding duplication of effort by calling numeric kernels with block size chosen so that overflow is guaranteed not to occur and exact results are provided. Other efforts have been devoted to specialized coefficients domains, such as GF(2) [6, 7] and GF(3) [8], where domain specific optimizations, such as bit packing, bit slicing and table lookup have been used together with domain specific algorithms such as four Russians. These efforts have tended to focus on the domain specific optimizations and not necessarily memory hierarchy and architecture specific optimations that have been the focus of the numeric linear algebra community.

The BLIS (BLAS-like Library Instantiation Software) framework [2] is an effort to provide easy access to the optimizations used in fast matrix kernels. By rewriting a few key kernels, the user can take advantage of the framework for efficient use of the memory hierarchy and other architectural features. In this presentation we report on an investigation of the use of BLIS to develop matrix-matrix multiplication kernels over various exact coefficient domains.

References

[1] R. Clint Whaley, Antoine Petitet and Jack J. Dongarra, *Automated Empirical Optimization of Software and the ATLAS Project*, Parallel Computing, 27, pp. 3–35 (2001).

[2] Field G. Van Zee and Robert A. van de Geijn, *BLIS: A Framework for Rapidly Instantiating BLAS Functionality*, ACM Transactions on Mathematical Software, 41(3), pp. 1–33 (2015).

[3] Kazushige Goto and Robert A. van de Geijn, *High-performance implementation of the level-3 BLAS*, ACM Transactions on Mathematical Software, 35(1), pp. 1–14 (2008).

[4] Kazushige Goto and Robert A. van de Geijn, *Anatomy of High-Performance Matrix Multiplication*, ACM Transactions on Mathematical Software. 34(3), pp. 1–25 (2008).

[5] Jean-Guillaume Dumas and Pascal Giorgi and Clément Pernet, *Dense Linear Algebra over Word-Size Prime Fields: the FFLAS and FFPACK Packages*, ACM Transactions on Mathematical Software, 35(3), pp. 1–42 (2008).

[6] Martin Albrecht and Gregory Bard, *The M4RI Library – Version 20121224*, `http://m4ri.sagemath.org` (2012).

[7] Martin Albrecht, Gregory Bard, William Hart, *Algorithm 898: Efficient Multiplication of Dense Matrices over GF(2)*, ACM Transactions on Mathematical Software, 37 (1), pp. 1–14 (2010).

[8] "J-G. Dumas and T. Gautier and M. Giesbrecht and P. Giorgi and B. Hovinen and E. Kaltofen and B. D. Saunders and W. Turner and G. Villard, *Linbox: A Generic Library for Exact Linear Algebra*, in ICMS'02, pp. 40–50 (2002).

Sparse matrices in computer algebra when using distributed memory: theory and applications

G. Malaschonok[1], E. Ilchenko[2]

[1] *Tambov State University, Russia, malaschonok@gmail.com*
[2] *Tambov State University, Russia, ilchenkoea@gmail.com*

J. Dongarra at his talk at International Congress ICMS-2016 [1] put attansion on the several difficult challenges. The task of managing calculations on a cluster with distributed memory for algorithms with sparse matrices is today one of the most difficult challenges.

Here we must also add problems with the type of the basic algebra: matrices can be over fields or over commutative rings. For sparse matrices, it is not true that all computations over polynomials or integers can be reduced to computations in finite fields. Such reduction may be not effective for sparse matrices.

We consider the class of block-recursive matrix algorithms. The most famous of them are standard and Strassen's block matrix multiplication, Schur and Strassen's block-matrix inversion [2].

Class of block-recursive matrix algorithms

Block-recursive algorithms were not so important as long as the calculations were performed on computers with shared memory. The generalization of Strassen's matrix inversion algorithm [2] with additional permutations of rows and columns by J. Bunch and J. Hopkroft [3] is not a block-recursive algorithm. Only in the nineties it became clear that block-recursive matrix algorithms are required to operate with sparse super large matrices on a supercomputer with distributed memory.

The block recursive algorithm for the solution of systems of linear equations and for adjoint matrix computation which is some generalisation of Schur inversion in commutative domains was discraibed in [7], [8] and [10]. See also at the book [9]. However, in all these algorithms, except matrix multiplication, a very strong restriction are imposed on the matrix. The leading minors, which are on the main diagonal, should not be zero.

This restriction was removed later. The algorithm that computes the adjoint matrix, the echelon form, and the kernel of the matrix operator for the commutative domains was proposed in [11]. The block-recursive algorithm for the Bruhat decomposition and the LDU decomposition for the matrix over the field was obtained in [12], and these algorithms were generaized for the matrices over commutative domains in [14] and in [15].

Some important areas of sparse matrix applications

Calculation of electronic circuits

The behavior of electronic circuits can be described by Kirchhoff's laws. The three basic approaches in this theory are direct current, constant frequency current and a current that varies with time. All these cases require the compilation and solution of sparse systems of equations (numerical, polynomial or differential). The solution of such differential equations by the Laplace method also leads to the solution of polynomial systems of equations [16].

Control systems

In 1967 Howard H. Rosenbrock introduced a useful state-space representation and transfer function matrix form for control systems, which is known as the Rosenbrock System Matrix [17]. Since that time, the properties of the matrix of polynomials being intensively studied in the literature of linear control systems.

Groebner basis.

Another important application is the calculation of Gröbner bases. A matrix composed of Buchberger S-polynomials is a strongly sparse matrix. Reduction of the polynomial system is performed when calculating the echelon and diagonal forms of this matrix. The algorithm F4 [18] was the first such matrix algorithm.

Solving ODE's and PDEâs.

Solving ODE's and PDE's is often based on solution of leanear systems with sparse matrices over numbers or over polynomials. One of the important class of sparse matrix is called quasiseparable. Any submatrix of quasiseparable matrix entirely below or above the main diagonal has small rank. These quasiseparable matrices arise naturally in solving PDEâs for particle interaction with the Fast Multi-pole Method (FMM). The efficiency of application of the block-recursive algorithm of the Bruhat decomposition to the quasiseparable matrices is studied in [20].

Development of the matrix recursive agorithms in integral domain

Algorithms for solution of a system of linear equations of size n in an integral domain, which served as the basis for creating recursive algorithms

(1983) Forward and backward algorithm ($\sim n^3$) [4].
(1989) One pass algorithm ($\sim \frac{2}{3}n^3$) [5].
(1995) Combined algoritm with upper left block of size r ($\sim \frac{7}{12}n^3$ for $r = \frac{n}{2}$) [6].

Recursive algorithms for solution of a system of linear equations and for adjoint matrix computation in an integral domain without permutations

(1997) Recursive algorithm for solution of a system of linear equations [7].
(2000) Adjoint matrix computation (with 6 levels) [8].
(2006) Adjoint matrix computation alternative algorithm (with 5 levels) [10].

Main recursive algorithms for sparse matrices

(2008) Computation of adjoint and inverse matrices and the operator kernel [11].
(2010) Bruhat and LEU decompositions in the feilds [12].
(2012) Bruhat and LDU decompositions in the domains [13], [14].
(2015) Bruhat and LDU decompositions in the domains (alternative algorithm) [15].

New achivements

(2013) It is proved that the LEU algorithm in the feild has the complexity $O(n^2 r^{\beta-2})$ for matrices of rank r. [19].
(2017) It is proved that the LEU algorithm in the feild has the complexity $O(n^2 s^{\beta-2})$ for quasiseparable matrix, if any it's submatrix which entirely below or above the main diagonal has small rank s [20].

Sparse matrices when using distributed memory

The block-recursive matrix algorithms for sparse matrix require a special approachs to managing parallel programs. One approach to the cluster computations management is a scheme with one dispatcher (or one master).

We consider another scheme of cluster menagement. It is a scheme with multidispatching, when each involved computing module has its own dispatch thread and several processing threads [21], [22].

We demonstrate the results of experiments with parallel programms on the base of multidispatching.

References

[1] Dongarra J. *With Extrim Scale Computing the Rules Have Changed.* In Mathematical Software. ICMS 2016, 5th International Congress, Procdistributed memoryeedings (G.-M. Greuel, T. Koch, P. Paule, A. Sommese, eds.), Springer, LNCS, volume 9725, pp. 3-8, (2016)

[2] *Strassen V. Gaussian Elimination is not optimal.* Numerische Mathematik. V. 13, Issue 4, 354–356 (1969)

[3] Bunch J., Hopkroft J. *Triangular factorization and inversion by fast matrix multiplication.* Mat. Comp. V. 28, 231-236 (1974)

[4] Malaschonok G.I. *Solution of a system of linear equations in an integral domain,* Zh. Vychisl. Mat. i Mat. Fiz. V.23, No. 6, 1983, 1497-1500, Engl. transl.: USSR J. of Comput. Math. and Math. Phys., V.23, No. 6, 497-1500. (1983)

[5] G.I. Malaschonok. *Algorithms for the solution of systems of linear equations in commutative rings.* Effective methods in Algebraic Geometry, Progr. Math., V. 94, Birkhauser Boston, Boston, MA, 1991, 289-298. (1991)

[6] G.I. Malaschonok. *Algorithms for computing determinants in commutative rings.* Diskret. Mat., 1995, Vol. 7, No. 4, 68-76. Engl. transl.: Discrete Math. Appl., Vol. 5, No. 6, 557-566 (1995).

[7] Malaschonok G. *Recursive Method for the Solution of Systems of Linear Equations.* Computational Mathematics. A. Sydow Ed, Proceedings of the 15th IMACS World Congress, Vol. I, Berlin, August 1997), Wissenschaft & Technik Verlag, Berlin, 475-480. (1997)

[8] Malaschonok G. *Effective Matrix Methods in Commutative Domains*, Formal Power Series and Algebraic Combinatorics, Springer, Berlin, 506-517. (2000)

[9] Malaschonok G. *Matrix computational methods in commutative rings.* Tambov, TSU, 213 p. (2002)

[10] Akritas A.G., Malaschonok G.I. *Computation of Adjoint Matrix.* Computational Science, ICCS 2006, LNCS 3992, Springer, Berlin, 486-489.(2006)

[11] Malaschonok G. *On computation of kernel of operator acting in a module* Vestnik Tambovskogo universiteta. Ser. Estestvennye i tekhnicheskie nauki [Tambov University Reports. Series: Natural and Technical Sciences], vol. 13, issue 1,129-131 (2008)

[12] Malaschonok G. *Fast Generalized Bruhat Decomposition.* Computer Algebra in Scientific Computing, LNCS 6244, Springer, Berlin 2010. 194-202. distributed memory DOI 10.1007/978-3-642-15274-0_16. arxiv:1702.07242 (2010)

[13] Malaschonok G. *On fast generalized Bruhat decomposition in the domains.* Tambov University Reports. Series: Natural and Technical Sciences. V. 17, Issue 2, P. 544-551. (http://parca.tsutmb.ru/src/MalaschonokGI17_2.pdf) (2012)

[14] Malaschonok G. *Generalized Bruhat decomposition in commutative domains.* Computer Algebra in Scientific Computing. CASC'2013. LNCS 8136, Springer, Heidelberg, 2013, 231-242. DOI 10.1007/978-3-319-02297-0_20. arxiv:1702.07248 (2013)

[15] Malaschonok G., Scherbinin A. *Triangular Decomposition of Matrices in a Domain.* Computer Algebra in Scientific Computing. LNCS 9301, Springer, Switzerland, 2015, 290-304. DOI 10.1007/978-3-319-24021-3_22. arxiv:1702.07243 (2015)

[16] Paul, Clayton R. *Fundamentals of Electric Circuit Analysis.* John Wiley & Sons. (2001). ISBN 0-471-37195-5.

[17] Rosenbrock, H.H. *Transformation of linear constant system equations.* Proc. I.E.E. V.114, 541â544. (1967)

[18] Faugere, J.-C. *A new efficient algorithm for computing Gröbner bases (F4)* . Journal of Pure and Applied Algebra. Elsevier Science. Vol. 139, N.1, 61-88. (1999)

[19] Dumas, J.-G., Pernet, C., Sultan, Z. *Simultaneous computation of the row and column rank profiles.* In: Kauers, M. (Ed.), Proc. ISSACâ13. ACM Press, pp. 181-188. (2013)

[20] Pernet C., Storjohann A. *Time and space efficient generators for quasiseparable matrices.* arXiv:1701.00396 (2 Jan 2017) 29 p. (2017)

[21] Ilchenko E.A. *An algorithm for the decentralized control of parallel computing process.* Tambov University Reports. Series: Natural and Technical Sciences, Vol. 18, No. 4, 1198-1206 (2013)

[22] Ilchenko E.A. *About effective methods parallelizing block recursive algorithms.* Tambov University Reports. Series: Natural and Technical Sciences, Vol. 20, No. 5, 1173-1186 (2015)

Comprehensive Optimization of Parametric Kernels for Graphics Processing Units

Xiaohui Chen[1], Marc Moreno Maza[2], Jeeva Paudel[3], Ning Xie[4]

[1] *AMD, Markham, Ontario, Canada*
[2] *U. Western Ontario, London, Ontario, Canada* moreno@csd.uwo.ca
[3] *IBM Canada Ltd, Markham, Ontario, Canada*
[4] *Huawei Technologies Canada, Markham, Ontario, Canada*

Overview

It is well-known that the advent of hardware acceleration technologies (multicore processors, graphics processing units, field programmable gate arrays) provide vast opportunities for innovation in computing. In particular, GPUs combined with *low-level heterogeneous programming models*, such as CUDA (the *Compute Unified Device Architecture*, see [17, 2]), brought super-computing to the level of the desktop computer. However, these low-level programming models carry notable challenges, even to expert programmers. Indeed, fully exploiting the power of hardware accelerators by writing CUDA code often requires significant code optimization effort. While such effort can yield high performance, it is desirable for many programmers to avoid the explicit management of the hardware accelerator, e.g. data transfer between host and device, or between memory levels of the device. To this end, *high-level* models for accelerator programming, notably OpenMP [10, 4] and OpenACC [21, 3], have become an important research direction. With these models, programmers only need to annotate their C/C++ (or FORTRAN) code to indicate which portion of code is to be executed on the device, and how data is mapped between host and device.

In OpenMP and OpenACC, the division of the work between thread blocks within a grid, or between threads within a thread block, can be expressed in a loose manner, or even ignored. This implies that code optimization techniques must be applied in order to derive efficient CUDA code. Moreover, existing software packages (e.g. PPCG [22], C-to-CUDA [6], HiCUDA [13], CUDA-CHiLL [14]) for generating CUDA code from annotated C/C++ programs, either let the user choose, or make assumptions on, the characteristics of the targeted hardware, and on how the work is divided among the processors of that device. These choices and assumptions limit *code portability* as well as opportunities for *code optimization*.

To deal with these challenges in translating annotated C/C++ programs to CUDA, we propose in [8] to generate *parametric* CUDA *kernels*, that is, CUDA

kernels for which program parameters (e.g. number of threads per thread block) and machine parameters (e.g. shared memory size) are symbolic entities instead of numerical values. Hence, the values of these parameters need not to be known during code generation: machine parameters can be looked up when the generated code is loaded on the target machine, while program parameters can be deduced, for instance, by auto-tuning.

A proof-of-concept implementation, presented in [8] and publicly available[1], uses another high-level model for accelerator programming, called METAFORK, that we introduced in [9]. The experimentation shows that the generation of parametric CUDA kernels can lead to significant performance improvement w.r.t. approaches based on the generation of CUDA kernels that are *not* parametric. Moreover, for certain test-cases, our experimental results show that the optimal choice for program parameters may depend on the input data size.

In this work, our goal is to enhance the framework initiated in [8] by generating *optimized* parametric CUDA kernels. As we shall see, this can be done in the form of a case discussion, based on the possible values of the machine and program parameters. The output of a procedure generating optimized parametric CUDA kernels will be called a *comprehensive parametric* CUDA *kernel*. A simple example is shown on Figure 2. In broad terms, this is a decision tree where:

1. each internal node is a Boolean condition on the machine and program parameters, and
2. each leaf is a CUDA program $\mathscr{P}$, optimized w.r.t. prescribed criteria and optimization techniques, under the conjunction of the conditions along the path from the root of the tree to $\mathscr{P}$.

The intention, with this concept, is to automatically generate optimized CUDA kernels from annotated C/C++ code without knowing the numerical values of some or even any of the machine and program parameters. This naturally leads to case distinction depending on the values of those parameters, which materializes into a disjunction of conjunctive non-linear polynomial constraints. Symbolic computation is the natural framework for manipulating such systems of constraints; our `RegularChains` library[2] provides the appropriate algorithmic tools for that task.

Other research groups have approached the questions of *code portability* and *code optimization* in the context of CUDA code generation from high-level programming models. They use techniques like auto-tuning [12, 14], dynamic instrumentation [15] or both [20]. Rephrasing [14], "those techniques explore empirically different data placement and thread/block mapping strategies, along with

[1] `www.metafork.org`

[2] This library, shipped with the commercialized computer algebra system MAPLE, is freely available at `www.regularchains.org`.

other code generation decisions, thus facilitating the finding of a high-performance solution."

In the case of auto-tuning techniques, which have been used successfully in the celebrated projects ATLAS [23], FFTW [11], and SPIRAL [18], part of the code optimization process is done *off-line*, that is, the input code is analyzed and an optimization strategy (i.e a sequence of composable code transformations) is generated, and then applied on-line (i.e. on the targeted hardware). We propose to push this idea further by applying the optimization strategy off-line, thus, even before the code is loaded on the targeted hardware.

We conclude this extended abstract with an example illustrating the notion of comprehensive parametric CUDA kernels, along with a procedure to generate them. Our input is the for-loop nest of Figure 1 which computes the sum of two matrices `b` and `c` of order N using a blocking strategy; each matrix is divided into blocks of format $\texttt{B0} \times \texttt{B1}$. This input code is annotated for parallel execution in the METAFORK language. The body of the statement `meta_schedule` is meant to be offloaded to a GPU device and each meta_for loop is a parallel for-loop where all iterations can be executed concurrently.

```
int dim0 = N/B0, dim1 = N/(2*B1);
meta_schedule {
  meta_for (int v = 0; v < dim0; v++)
    meta_for (int p = 0; p < dim1; p++)
      meta_for (int u = 0; u < B0; u++)
        meta_for (int q = 0; q < B1; q++) {
          int i = v * B0 + u;
          int j = p * B1 + q;
          if (i < N && j < N/2) {
            c[i][j] = a[i][j] + b[i][j];
            c[i][j+N/2] =
               a[i][j+N/2] + b[i][j+N/2];
          }
        }
}
```

Figure 1: A `meta_for` loop nest for adding two matrices.

We make the following simplistic assumptions for the translation of this for-loop nest to CUDA.

1. The target machine has two parameters: the maximum number R of registers per thread, and the maximum number T of threads per thread-block; all other hardware limits are ignored.
2. The generated kernels depend on two program parameters, B_0 and B_1, which

define the format of a 2D thread-block.

3. The optimization strategy (w.r.t. register usage per thread) consists in reducing the work per thread (by reducing loop granularity).

A possible comprehensive parametric CUDA kernel is given by the pairs (C_1, K_1) and (C_2, K_2), where C_1, C_2 are two sets of algebraic constraints on the parameters and K_1, K_2 are two CUDA kernels that are optimized under the constraints respectively given by C_1, C_2, see Figure 2. The following computational steps yield the pairs (C_1, K_1) and (C_2, K_2).

(S1) The METAFORK code is mapped to an intermediate representation (IR) say that of LLVM[3], or alternatively, to PTX[4] code.

(S2) Using this IR (or PTX) code, one *estimates* the number of registers that a thread requires; on this example, using LLVM IR, we obtain an estimate of 14.

(S3) Next, we apply the optimization strategy, yielding a new IR (or PTX) code, for which register pressure reduces to 10. Since no other optimization techniques are considered, the procedure stops with the result shown on Figure 2.

Note that, strictly speaking, the kernels K_1 and K_2 on Figure 2 should be given by PTX code. But for simplicity, we are presenting them by counterpart CUDA code.

$$C_1 : \begin{cases} B_0 \times B_1 \leq T \\ 14 \leq R \end{cases} \qquad C_2 : \begin{cases} B_0 \times B_1 \leq T \\ 10 \leq R < 14 \end{cases}$$

```
__global__  void K1(int *a, int *b, int *c,
                                  int B0, int B1) {
     int i = blockIdx.y * B0 + threadIdx.y;
     int j = blockIdx.x * B1 + threadIdx.x;
     if (i < N && j < N/2) {
        a[i*N+j] = b[i*N+j] + c[i*N+j];
        a[i*N+j+N/2] = b[i*N+j+N/2] + c[i*N+j+N/2];
     }
}
dim3 dimBlock(B1, B0);
dim3 dimGrid(N/(2*B1), N/B0);
K1 <<<dimGrid, dimBlock>>> (a, b, c, N, B0, B1);
```

```
__global__  void K2(int *a, int *b, int *c, int N,
                                  int B0, int B1) {
     int i = blockIdx.y * B0 + threadIdx.y;
     int j = blockIdx.x * B1 + threadIdx.x;
     if (i < N && j < N)
        a[i*N+j] = b[i*N+j] + c[i*N+j];
}
dim3 dimBlock(B1, B0);
dim3 dimGrid(N/B1, N/B0);
K2 <<<dimGrid, dimBlock>>> (a, b, c, N, B0, B1);
```

Figure 2: A comprehensive parametric CUDA kernel for matrix addition.

While this was a *toy-example*, advanced test cases can be found in Chapter 7 of the PhD thesis of the first author at

`http://ir.lib.uwo.ca/etd/4429`

[3] Quoting Wikipedia: "The LLVM compiler infrastructure project (formerly Low Level Virtual Machine [16, 7]) is a framework for developing compiler front ends and back ends".

[4] The *Parallel Thread Execution* (PTX) [5] is the pseudo-assembly language to which CUDA programs are compiled by NVIDIA's NVCC compiler. PTX code can also be generated from (enhanced) LLVM IR, using nvptx back-end [1], following the work of [19].

Acknowledgments

The authors would like to thank the IBM Toronto Labs and NSERC of Canada for supporting their work.

References

[1] User guide for NVPTX. The LLVM Compiler Infrastructure. `http://llvm.org/docs/NVPTXUsage.html#introduction`.

[2] CUDA runtime API: v7.5. NVIDIA Corporation, 2015. `http://docs.nvidia.com/cuda/pdf/CUDA_Runtime_API.pdf`.

[3] The OpenACC application programming interface. OpenACC-Standard.org, 2015.

[4] OpenMP application program interface version 4.5. OpenMP Architecture Review Board, 2015. `http://www.openmp.org/mp-documents/openmp-4.5.pdf`.

[5] Parallel thread execution ISA : v4.3. NVIDIA Corporation, 2015. `http://docs.nvidia.com/cuda/pdf/ptx_isa_4.3.pdf`.

[6] M. Baskaran, J. Ramanujam, and P. Sadayappan. Automatic C-to-CUDA code generation for affine programs. In *Proceedings of CC'10/ETAPS'10*, pages 244–263, Berlin, Heidelberg, 2010. Springer-Verlag.

[7] Carlo Bertolli, Samuel F. Antao, Alexandre E. Eichenberger, Kevin O'Brien, Zehra Sura, Arpith C. Jacob, Tong Chen, and Olivier Sallenave. Coordinating GPU threads for OpenMP 4.0 in LLVM. In *Proceedings of LLVM-HPC '14*, pages 12–21. IEEE Press, 2014.

[8] Changbo Chen, Xiaohui Chen, Abdoul-Kader Keita, Marc Moreno Maza, and Ning Xie. MetaFork: A compilation framework for concurrency models targeting hardware accelerators and its application to the generation of parametric CUDA kernels. In *Proceedings of CASCON 2015*, pages 70–79, 2015.

[9] Xiaohui Chen, Marc Moreno Maza, Sushek Shekar, and Priya Unnikrishnan. MetaFork: A framework for concurrency platforms targeting multicores. In *Processing of IWOMP 2014*, pages 30–44, 2014.

[10] Leonardo Dagum and Ramesh Menon. OpenMP: An industry standard API for shared-memory programming. *Computational Science & Engineering, IEEE*, 5(1):46–55, 1998.

[11] Matteo Frigo and Steven G. Johnson. FFTW: an adaptive software architecture for the FFT. In *Proceedings of ICASSP*, pages 1381–1384. IEEE, 1998.

[12] Scott Grauer-Gray, Lifan Xu, Robert Searles, Sudhee Ayalasomayajula, and John Cavazos. Auto-tuning a high-level language targeted to GPU codes. In *Innovative Parallel Computing*. IEEE, 2012.

[13] Tianyi David Han and Tarek S. Abdelrahman. hiCUDA: A high-level directive-based language for GPU programming. In *Proceedings of GPGPU-2*, pages 52–61. ACM, 2009.

[14] Malik Khan, Protonu Basu, Gabe Rudy, Mary Hall, Chun Chen, and Jacqueline Chame. A script-based autotuning compiler system to generate high-performance CUDA code. *ACM Trans. Archit. Code Optim.*, 9(4):31:1–31:25, January 2013.

[15] Thomas Kistler and Michael Franz. Continuous program optimization: A case study. *ACM Trans. on Programming Languages and Systems*, 25(4):500–548, 2003.

[16] Chris Lattner and Vikram Adve. LLVM: A compilation framework for lifelong program analysis & transformation. In *Proceedings of CGO '04*, pages 75–. IEEE Computer Society, 2004.

[17] J. Nickolls, I. Buck, M. Garland, and K. Skadron. Scalable parallel programming with CUDA. *Queue*, 6(2):40–53, 2008.

[18] Markus Püschel, José M. F. Moura, Bryan Singer, Jianxin Xiong, Jeremy R. Johnson, David A. Padua, Manuela M. Veloso, and Robert W. Johnson. Spiral: A generator for platform-adapted libraries of signal processing alogorithms. *IJHPCA*, 18(1), 2004.

[19] Helge Rhodin. A PTX code generator for LLVM. Master's thesis, Saarland University, 2010.

[20] Chenchen Song, Lee-Ping Wang, and Todd J Martínez. Automated code engine for graphical processing units: Application to the effective core potential integrals and gradients. *Journal of chemical theory and computation*, 2015.

[21] Xiaonan Tian, Rengan Xu, Yonghong Yan, Zhifeng Yun, Sunita Chandrasekaran, and Barbara M. Chapman. Compiling a high-level directive-based programming model for GPGPUs. In *Languages and Compilers for Parallel Computing - 26th Int. Work.* Springer, 2013.

[22] S. Verdoolaege, J. Carlos Juega, A. Cohen, J. Ignacio Gómez, C. Tenllado, and F. Catthoor. Polyhedral parallel code generation for CUDA. *TACO*, 9(4):54, 2013.

[23] R. Clinton Whaley and Jack Dongarra. Automatically tuned linear algebra software. In *PPSC*, 1999.

Session 16

General session

Session chairs:

Michael Wester
University of New Mexico, USA

Stanly Steinberg
University of New Mexico, USA

The FunctionAdvisor: extending information on mathematical functions with computer algebra algorithms

E.S. Cheb-Terrab[1]

[1] *Maplesoft R&D, Canada, ecterrab@maplesoft.ca*

A shift in paradigm is happening, from: encoding information into a database, to: encoding essential blocks of information *together with algorithms* within a computer algebra system; so that the information is not only searchable but can also be recreated in many different ways, as well as actually used to compute. This talk focuses on this shift in paradigm over a real case example: the digitizing of information regarding mathematical functions as *the FunctionAdvisor* project of the Maple computer algebra system. Examples of algorithms at work, for differential polynomial representations, nth order symbolic differentiation, and computation of branch cuts of arbitrary algebraic expressions, as well as a network of relations between mathematical functions, all this extending the information typically found in textbooks like Abramowitz and Stegun, are shown.

References

[1] E.S. Cheb-Terrab, *The Function Wizard project: A Computer Algebra Handbook of Special Functions*. Proceedings of the Maple Summer Workshop. University of Waterloo, Canada (2002).

[2] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions*, Dover (1964).

[3] F.W.J. Olver, D.W. Lozier, R.F. Boisvert, C.W. Clark, *NIST Handbook of Mathematical Functions*, Cambridge University Press (2010).

The four double-hypergeometric Appell functions, a complete implementation in a computer algebra system

E.S. Cheb-Terrab[1]

[1] *Maplesoft R&D, Canada, ecterrab@maplesoft.ca*

The four multi-parameter Appell functions, AppellF1, AppellF2, AppellF3, and AppellF4 are double hypergeometric functions that vastly extend the 2F1 hypergeometric and some cases of the MeijerG functions, and through them also include as particular cases most of the known functions of mathematical physics. These Appell functions have been popping up with increasing frequency in applications in quantum mechanics, molecular physics, and general relativity. In this talk, a full implementation of these functions in the Maple computer algebra system, including, for the first time, their numerical evaluation over the whole complex plane, is presented, with details about the symbolic and numerical strategies used.

References

[1] P. Appell, J. Kampe de Feriet, *Fonctions Hypergeometriques et hyperspheriques*, Gauthier-Villars (1926).

[2] H. M. Srivastava, P. W. Karlsson, *Multiple Gaussian Hypergeometric Series*, Ellis Horwood (1985).

The International Mathematical Knowledge Trust

Ingrid Daubechies[1], Patrick Ion[2], Stephen M. Watt[3]

[1] *Duke University, Durham NC, USA ingrid@duke.edu*
[2] *Mathematical Reviews, Ann Arbor MI, USA pion@umich.edu*
[3] *University of Waterloo Waterloo, Canada smwatt@uwaterloo.ca*

A long-term goal, espoused by the International Mathematical Union (IMU) a decade ago, has been to make available the totality of mathematical knowledge in digital form, with human- and machine-usable tools to build on that knowledge. This talk presents the steps being taken by an IMU working group toward this goal.

It is essential to have an organization so that the attempts the global task of making mathematical knowledge better available. Projects that serve this goal, those already underway and those proposed in the immediate future, can then be brought together as whole, providing a public good for the world. Without such coordination, many useful initiatives have limited lives and the work they have done may be lost or duplicate other projects.

The organization, which we call the International Mathematical Knowledge Trust (IMKT), is being set up to coordinate contributing participants working toward the Global Digital Mathematics Library. The immediate objectives, in the first year, are to create the not-for-profit organization, establish its boards and governance, to set out suitable technical frameworks for cooperative development, and to undertake seed projects.

More than any other field, mathematical knowledge is unique in its precision and its enduring utility. The literature containing this mathematical knowledge is, however, widely dispersed, uses a variety of inconsistent conventions and notations, and for the most part is not in a form that admits automated use. Few except disciplinary experts can combine results from several papers and be sure of the results' correctness and consistency. The correct and reliable application of sequences of mathematical results lies at the heart of our ever-expanding technical infrastructure. Advances here propel our society. Errors can cause disasters.

The long-term plans must address this issue from both the technical and the organizational sides. The technical questions are such as

- "How can the existing literature repositories be united?",
- "What forms of semantic representation are most achievable and useful for mathematical knowledge?",
- "How can mathematical OCR and natural language processing be used in a semi-supervised machine learning bootstrap process?"

The organizational side addresses questions such as

- "How can we build upon existing research projects around the globe?"
- "How can we most effectively engage relevant commercial enterprises including publishers and software companies?"
- "How can these efforts be brought to the public in a coherent and sustainable fashion?"

There are compelling arguments to create a comprehensive knowledge base from the mathematical literature. The present organizational environment of mathematics seems to have been largely hostile to development of significant open data resources in mathematics. This leaves an organizational vacuum which we propose be filled by the IMKT, with moral support from the IMU (International Mathematical Union). The hope is that IMKT may incrementally grow a prospering network of open mathematical knowledge providers, a union of which will provide the long-awaited global digital mathematics library.

How a code for verifying our conjecture opened new directions -Abstract

Eli Bagno

May 22, 2017

Abstract

A common tool used in enumerating combinatorial objects is the generating function, which is an algebraic way of presenting all the enumerative information in one glance. When the generating function is a polynomial which can be factorized, the factorization may provide important information about the objects themselves. Nowadays many mathematicians use computer code to test their conjectures before attempting to prove them in a rigorous form. While trying to find a closed formula for the length function of a certain group of symmetries, we used a Sage code to obtain a polynomial generating function. When we then used Mathematica to factorize this polynomial, the results provided us with a very significant insight: the formula we were looking for must consist of two parts, corresponding to a specific known decomposition of the group into cosets.

1 Complex reflection groups

Let S_n be the symmetric group on n letters $1, \ldots, n$. For $\sigma \in S_n$ with $\sigma(i) = r_i$, $1 \leq i \leq n$, we denote by $((a_1, \ldots, a_n), (r_1, \ldots, r_n)$ the $n \times n$ monomial matrix with non-zero entries a_i in the $(i, r_i)-$ positions. For $p|m$ in $\mathbb{N}$, we set:

$$G(r, p, n) = \{((a_1, \ldots, a_n), \sigma) \in GL_n(\mathbb{C}) \mid a_i^r = 1\}.$$

We denote an element of $G(r, p, n)$ in a more concise manner:

$$(\sigma, k) = a_1^{k_1} \cdots a_n^{k_n}$$

for $\sigma = a_1 \cdots a_n$ and $k = (k_1, \ldots, k_n)$.

Example 1.1.

$$\pi = (312, (1, 3, 3)) = 3^1 1^3 2^3$$

Various sets of generators have been defined for complex reflection groups but (as far as we know), no length function has been formulated.

In a separate paper [1] we provide such a function for the case of $G(r, r, n)$ with a specific choice of generating set proposed by Shi. (See [2]).

1.1 Shi's Generators for $G(r,r,n)$

For each $i \in \{1,\ldots,n-1\}$ let $s_i = (i, i+1)$ be the well-known adjacent transpositions generating S_n.

Define $t_0 = (1^{r-1}, n^1)$. In [2] the following theorem is proven.

Theorem 1.2. *The set* $\{t_0, s_1, \ldots, s_{n-1}\}$ *generates* $G(r,r,n)$.

After we found a length function for the elements of the group $G(r,r,n)$, we proceeded to seek a generating function. In order to be able to get a grasp on the form that generating function should take, we composed a simple Sage program which went over all the elements of $G(r,r,n)$ for some small values of r and n and calculated the length, using the length function we had discovered. When we used the Mathematica program to factor the resulting polynomial, we found out that in all the cases which had been checked, the factor $[n]_q! = (1+q)(1+q+q^2)\cdots(1+q+\cdots+q^{n-1})$ appeared. Here are two examples of the factorizations we have obtained:

Example 1.3.

$$G_{4,4,4}(q) = [4]_q!(1+2q^2+3q^3+4q^4+5q^5+7q^6+8q^7+10q^8+12q^9+7q^{10}+3q^{11}).$$

Example 1.4.

$$G_{6,6,3}(q) = [3]_q!(1+q+2q^2+2q^3+3q^4+3q^5+4q^6+4q^7+5q^8+5q^9+6q^{10}).$$

Since $[n]_q!$ is the generating function of the length function of S_n, these and other examples led us to the conclusion that the correct way of presenting the length function for the elements of $G(r,r,n)$ must be based on a decomposition of $G(r,r,n)$ into cosets of S_n.

In [1] we provide the following length function for $G(r,r,n)$.

Theorem 1.5. *Let* $\pi = a_1^{k_1}\cdots a_n^{k_n} \in G(r,r,n)$.

Write $\pi = u\cdot\sigma$ *where* $u \in S_n$ *and* σ *is the minimal length representative. Then:* $\ell(\pi) = \sum_{1\le i<j\le n} |k_j - k_i| - noninv(k) + inv(u)$

References

[1] E. Bagno and M. Novick, *A length function for the complex reflection group* $G(r,r,n)$, in preparation.

[2] J. Y. Shi, *Certain imprimitive reflection groups and their generic versions*, Transcations of the A.M.S., Vol. 364, No. 5, pp. 2115-2129.

Using Gröbner basis theory for an interval method solving underdetermined equations systems

Bartłomiej Jacek Kubica[1]

[1] *Department of Applied Informatics, Warsaw University of Life Sciences, Poland, bartlomiej_kubica@sggw.pl*

Let us consider solving the nonlinear underdetermined system of equations:

$$f\colon X \to \mathbb{R}^m, \text{ where } X \subseteq \mathbb{R}^n,\ n \geq m\ . \tag{1}$$

Interval methods (see, e.g., [6]) have proven to be useful, in particular, in solving nonlinear systems of type (1). One of their advantages is allowing not only to locate all solutions of underdetermined systems; i.e., the whole solution manifold can be enclosed by a set of boxes (typically we compute two sets: of verified and possible solutions, cf., e.g., [9]).

Due to the nature of interval arithmetic, it is pretty important, what formulae we compute in it. The simplest example is $[\underline{x}, \overline{x}] - [\underline{x}, \overline{x}]$, which, according to the rules of interval arithmetic is equal to $[\underline{x} - \overline{x}, \overline{x} - \underline{x}]$ and it is in general different from zero.

It might be unlikely that we found a $\boldsymbol{x} - \boldsymbol{x}$ in our formulae, but also $\boldsymbol{x}^2 + \boldsymbol{x}$, $\boldsymbol{x} \cdot (\boldsymbol{x} + 1)$ and $(\boldsymbol{x} + \frac{1}{2})^2 - \frac{1}{2}$, obviously equivalent for real numbers, may have different results for an interval argument.

Hence, combining interval methods with some symbolic transformations might be very worthwhile.

Benhamou et alii were, to the best knowledge of the author, the first ones to propose preprocessing equations systems under consideration using the Gröbner basis theory [2], [3]. Computing the Gröbner basis of a set of polynomials, corresponding to the equation system, in lexicographic order $x_1 \prec x_2 \prec \cdots \prec x_n$, results in a system in triangular form:

$$\begin{cases} p_1(x_1, x_2, \ldots, x_n) = 0 \\ \cdots \\ p_{n-1}(x_1, x_2) = 0 \\ p_n(x_1) = 0 \end{cases}\ .$$

Obviously, variables in the above ordering can be permuted, resulting in a different transformed system, but also in a triangular form.

The transformation thus allows us to reduce solving the whole system to subsequent solving of univariate equations: $p_n(x_1) = 0$, $p_2(x_1, x_2) = 0$, for

solutions x_1^* of the previous equation, etc. The procedure, according to the quoted papers is efficient. A similar idea has been applied by the author for solving optimization problems; see [7].

In all above cases, the system of transformed conditions gets reduced to the triangular form. It is not so for an underdetermined system of equations, where we only get the following transformed system:

$$\begin{cases} p_1(x_1, \ldots, x_{n-m+1}, \ldots, x_n) = 0, \\ \ldots \\ p_{m-1}(x_1, \ldots, x_{n-m+1}, x_{n-m+2}) = 0, \\ p_m(x_1, \ldots, x_{n-m+1}) = 0 \end{cases} .$$

Here, we need to start with solving a multivariate underdetermined equation $p_m(x_1, \ldots, x_{n-m+1}) = 0$. Let us denote the solution manifold of this equation $M = \{(x_1, \ldots, x_{n-m+1}) \mid p_m(x_1, \ldots, x_{n-m+1}) = 0\}$. We obtain M as a set of boxes enclosing its segments (cf., e.g., [9]).

For all these boxes, we can proceed with solving univariate equations to find the solution of the initial system (1), as in the well-determined case.

Computing M is obviously, much more demanding and cumbersome than solving a univariate equation, but still it is an improvement: instead of solving a system of m equations in n variables, we need to enclose the solution manifold of a single equation in $(n - m + 1)$ variables.

What is more, next steps, in which we compute feasible values of x_{n-m+2}, x_{n-m+3}, …, x_n can be parallelized in a pretty scalable manner: M is probably enclosed by a large number of boxes and computations for each of these boxes are independent on computations on the others.

To the best knowledge of the author, this approach has not been considered or tested for underdetermined systems of equations and this paper is going to fill this gap.

The solver used by the author is HIBA_USNE [5], written by himself and described, i.a., in [9], [10]. For symbolic preprocessing, CoCoALib [1] is applied.

References

[1] J. Abbott and A. M. Bigatti, *CoCoALib: a C++ library for doing Computations in Commutative Algebra*, `http://cocoa.dima.unige.it/cocoalib` (2017).

[2] F. Benhamou and L. Granvilliers, *Combining local consistency, symbolic rewriting and interval methods*, Artificial Intelligence and Symbolic Mathematical Computation, **1996**, pp. 144–159 (1996), `http://www.sciences.univ-nantes.fr/info/perso/permanents/benhamou/papers/BenGra_AISMC96.pdf`.

[3] F. Benhamou and L. Granvilliers, *Automatic generation of numerical redundancies for non-linear constraint solving*, Reliable Computing, **3**, 3, pp. 335–344 (1997), http://www.sciences.univ-nantes.fr/info/perso/permanents/benhamou/papers/BenGra_Reliable97.pdf.

[4] B. Buchberger, *Gröbner bases and systems theory*, Multidimensional Systems and Signal Processing, *12*, 3, pp. 223–251 (2001), http://www.risc.uni-linz.ac.at/people/buchberg/papers/2001-05-12-A.ps.

[5] *HIBA_ USNE*, C++ library, https://www.researchgate.net/publication/316687827_HIBA_USNE_Heuristical_Interval_Branch-and-prune_Algorithm_for_Underdetermined_and_well-determined_Systems_of_Nonlinear_Equations_-_Beta_25 (2017).

[6] R. B. Kearfott, *Rigorous Global Search: Continuous Problems*, Kluwer, Dordrecht, 1996.

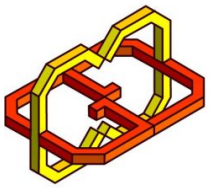
[7] B. J. Kubica and K. Malinowski, *An interval global optimization algorithm combining symbolic rewriting and componentwise Newton method applied to control a class of queueing systems*, Reliable Computing, **11**, 5, pp. 393–411 (2005).

[8] B.J. Kubica, *A class of problems that can be solved using interval algorithms*, Computing, **94**, pp. 271–280 (2012).

[9] B.J. Kubica, *Presentation of a highly tuned multithreaded interval solver for underdetermined and well-determined nonlinear systems*, Numerical Algorithms, **70**, 4, pp. 929–963 (2015).

[10] B.J. Kubica, *Parallelization of a bound-consistency enforcing procedure and its application in solving nonlinear systems*, Journal of Parallel and Distributed Computing, published online https://doi.org/10.1016/j.jpdc.2017.03.009 (2017).

Sponsors

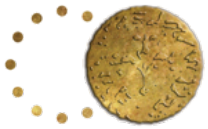


Center for Graphics and Geometric Computing
(CGGC)
Computer Science Department, Technion, Israel.

Israel
Mathematical
Union האגוד הישראלי
למתמטיקה

The Emmy Noether
Mathematical Institute
A Minerva Center

Computer Algebra Research Group
of
Wilfrid Laurier University



THE JERUSALEM DEVELOPMENT AUTHORITY