C U R S O S E C O N G R E S O S

Proceedings

Santiago de Compostela,
June, 18-22, 2018

24th Conference on Applications of Computer Algebra - ACA 2018

Edited by
Francisco Botana
Felipe Gago
Manuel Ladra

Universidade
de Santiago
de Compostela
publicacións

24th Conference on Applications of Computer Algebra

ACA 2018

CURSOS E CONGRESOS DA
UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
Nº 248

Proceedings
Applications of Computer Algebra

Santiago de Compostela, Spain, June 18–22, 2018

Edited by
FRANCISCO BOTANA
FELIPE GAGO
MANUEL LADRA

2018
UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Edita
Servizo de Publicacións e Intercambio Científico
Campus Vida
15782 Santiago de Compostela
usc.es/publicacions

DOI: http://dx.doi.org/10.15304/9788416954872
ISBN 978-84-16954-87-2

Contents

Editors' introduction

Dear colleagues, It is our pleasure to welcome you to Santiago de Compostela for the 24^{th} Conference on Applications of Computer Algebra – ACA 2018.

The ACA conference series is devoted to promoting all manner of computer algebra applications, and encouraging the interaction of developers of computer algebra systems and packages with researchers and users (including scientists, engineers, educators, etc.). Topics include, but are not limited to, computer algebra in the sciences, engineering, medicine, pure and applied mathematics, education and computer science.

ACA Conferences are run in different Special Sessions. In ACA 2018, the following 12 Special Sessions have been accepted:

S01 General Session.

Organized by Michael Wester.

S02 Computer Algebra Modeling in Science and Engineering.

Organized by Alexander Prokopenya and Haiduke Sarafian.

S03 Computer Algebra in Education.

Organized by Michel Beaudin, Michael Wester, Alkis Akritas, Elena Varbanova, Noah Dana-Picard, Sara Hershkovitz and Anatoli Kouropatov.

S04 Applied and Computational Algebraic Topology.

Organized by Graham Ellis, Marian Mrozek, Aniceto Murillo, Pedro Real and Eduardo Sáenz de Cabezón.

S05 Computer Algebra for Dynamical Systems and Celestial Mechanics.

Organized by Victor Edneral, Nikolay Vassiliev and Aleksandr Mylläri.

S06 Computational Differential and Difference Algebra.

Organized by Vladimir Gerdt, Alexander Levin and Daniel Robertz.

S07 Algebraic and Algorithmic Aspects of Differential and Integral Operators.

Organized by Moulay Barkatou, Thomas Cluzeau, Georg Regensburger and Markus Rosenkranz.

S08 Dynamic Geometry and Mathematics Education.

Organized by Tomás Recio, Philippe R. Richard and M. Pilar Vélez.

S09 Computer Algebra in Coding Theory and Cryptography.

Organized by Irene Márquez Corbella and Emilio Suárez Canedo.

S10 Parametric Polynomial Systems.

Organized by Yosuke Sato and Katsusuke Nabeshima.

S11 Algorithms for Zero-Dimensional Ideals.

Organized by Vincent Neiger, Hamid Rahkooy and Éric Schost.

S12 Numerical Differential and Polynomial Algebra.

Organized by Greg Reid and Zahra Mohammadi.

From the very beginning, ACA Conferences have been a very important meeting point for professionals in the use of Computer Algebra in different fields. In this occasion, ACA 2018 has joined 120 participants from 25 different countries and 122 contributions have been accepted by session organizers.

This proceedings book contents abstracts of the 117 contributions presented at the conference, together with the four invited plenary talks and the sponsor presentation. When there are two o more authors, the name of the presenter is underlined.

The editors thank the organizers of the sessions for their good work and all the participants for their interest and contribution to make this meeting a very important event.

Santiago de Compostela, June 2018

The editors:
Francisco Botana
Felipe Gago
Manuel Ladra

Committees

- **General Chair**
  - Manuel Ladra, *University of Santiago de Compostela, Spain*
- **Program Chair**
  - Francisco Botana, *University of Vigo, Spain*
- **Publicity Chair**
  - Felipe Gago, *University of Santiago de Compostela, Spain*
- **Advisory Committee**
  - Stanly Steinberg, *Albuquerque, USA*
  - Michael Wester, *Albuquerque, USA*
  - Eugenio Roanes-Lozano, *University Complutense de Madrid, Spain*
- **Scientific Committee**
  - ACA working group
- **Local organizing committee**
  - Rafael Fernández-Casado
  - Alejandro Fernández-Fariña
  - Xabier García-Martínez
  - Pilar Paéz-Guillán

Invited Plenary Talks

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Applications of Computer Algebra to Verification and Satisfiability Checking

James H. Davenport[1]

Boolean Satisfiability Checking is one of the paradoxes of computer science: on the one hand it (as 3-SAT) is the quintessential NP-complete hard problem, on the other hand, problems with millions of instances are solved routinely. If we ask for (semi-)algebraic satisfiability over the reals, the quantified worst case complexity be-comes doubly exponential. While computer algebraists wrestle with this complexity, the Satisfiability Modulo Theories community has been working away pragmatically, using very different success criteria, and applying their techniques, especially in soft-ware and system verification. However, they could learn more from Computer Alge-bra, and we could learn from them. This talk will outline some of these directions.

[1]Department of Computer Sciences
University of Bath
Bath, United Kingdom
J.H.Davenport@bath.ac.uk

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

SAT Solvers and Computer Algebra Systems: A Powerful Combination for Mathematics

Vijay Ganesh[1]

In recent years we have witnessed a dramatic improvement in the performance of Boolean SAT solvers, despite the fact that the Boolean satisfiability problem is NP-complete [1, 2]. While SAT solvers are powerful combinatorial search algorithms, they are weak when it comes to domain-specific mathematical knowledge. On the other hand, computer algebra systems (CAS) are deep repositories of mathematical knowledge and contain many sophisticated mathematical algorithms. However, computer algebra systems are not as strong at combinatorial search as SAT solvers. Motivated by problems that require both powerful search and deep knowledge, we propose a SAT+CAS combination method that brings together the best of both these worlds aimed at solving problems in combinatorial mathematics.

In this talk I will present a SAT+CAS system, MathCheck [3, 4], that we developed and used to counterexample many combinatorial conjectures, most notably the Williamson conjecture. I will discuss the internals of MathCheck, how it can be used, and most importantly, how mathematicians can extend such SAT+CAS tools to tackle a variety of problems. I will also argue that we are witnessing a new long-term paradigmatic shift, wherein, previously unrelated methods such as solvers and CAS are being profitably combined to tackle hard mathematical problems.

Keywords: Boolean SAT solvers, Computer algebra systems, Combinatorial mathematics

Mathematics Subject Classification 2010: 68, 05

References

[1] Jia Hui Liang, Vijay Ganesh, Pascal Poupart, and Krzysztof Czarnecki. Learning Rate Based Branching Heuristic for SAT Solvers. In Proceedings of the 19^{th} International Conference on the Theory and Applications of Satisfiability Testing (SAT 2016), Bordeaux, France, July 5-8, 2016.
`https://sites.google.com/a/gsd.uwaterloo.ca/maplesat/`

[2] Jia Hui Liang, Hari Govind V K, Pascal Poupart, Krzysztof Czarnecki, and Vijay Ganesh. An Empirical Study of Branching Heuristics Through the Lens of Global Learning Rate. In Proceedings of the 20^{th} International Conference on Theory

and Applications of Satisfiability Testing (SAT 2017), Melbourne, Australia, Aug 28 - Sep 1, 2017.
https://sites.google.com/a/gsd.uwaterloo.ca/maplesat/

[3] Curtis Bright, Ilias Kotsireas, and Vijay Ganesh. A SAT+CAS Method for Enumerating Williamson Matrices of Even Order. In the Proceedings of the 32^{nd} AAAI Conference on Artificial Intelligence (AAAI 2018), New Orleans, USA, Feb 2-7, 2018.
https://sites.google.com/site/uwmathcheck/

[4] Ed Zulkoski, Curtis Bright, Albert Heinle, Ilias Kotsireas, Krzysztof Czarnecki, and Vijay Ganesh. Combining SAT Solvers with Computer Algebra Systems to Verify Combinatorial Conjectures. Journal of Automated Reasoning (JAR 2017), Volume 58, number 3, pages 313-339, 2017.
https://sites.google.com/site/uwmathcheck/

[1]Electrical and Computer Engineering Department
University of Waterloo
200 University Avenue West, Waterloo, Ontario, Canada N2L 3G1
Email: vganesh@uwaterloo.ca
Website: https://ece.uwaterloo.ca/~vganesh

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Dealing with real algebraic curves and surfaces for discovery: from experiments to theory and applications

Laureano Gonzalez-Vega[1]

Geometric entities such as the set of the real zeros of a bivariate equation or the image in of a rational parametrization can be treated algorithmically in a very efficient way by using a mixture of symbolic and numerical techniques. This implies that it is possible to know exactly which is the topology (connected components and their relative position, connectedness, singularities, etc.) of such a curve or surface if their equations are known in an exact manner (whatever this means) for moderate or high degrees. We would describe several different "experiments" coming from Algebraic Geodesy and Computer Aided Design that highlight how new visualisation tools in Computational Mathematics mixing symbolic and numerical techniques allow to perform experiments conveying either to mathematical discoveries and/or to new computational techniques useful in applications.

[1]Departamento de Matemáticas, Estadística y Computación
Universidad de Cantabria, Spain

laureano.gonzalez@unican.es

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Automatic Geometric Theorem Proving and Discovering Using (Comprehensive) Groebner Bases

Dingkang Wang[1]

Automatic geometric theorem proving and discovering is to prove and derive mathematical theorems by computer programs, which has been studied for several decades. It can be traced back to the great work of Tarski, Seidenberg, Gelernter,Collins,Wu and so on. The extensive study in this research field is due to the introduction of Wu's method in later 1970s, which is surprisingly efficient for proving difficult geometric theorem. First, I will introduce our work on discovering geometric theorems by using the comprehensive Groebner systems, i.e. finding some complementary conditions such that the geometric statement will become true under the original hypotheses and these complementary conditions. Particularly, efficient algorithms for computing comprehensive Groebner systems/bases are also reviewed. Second, I will investigate the problem whether the conclusion is true on some components of the hypotheses for a geometric statement. In that case, the affine variety associated with the hypotheses is reducible. A polynomial vanishes on some but not all the components of a variety if and only if it is a zero divisor in a quotient ring with respect to the radical ideal defined by the variety. Based on this fact, we present an algorithm to decide if a geometric statement is only true on components. Besides proving theorems, the parametrical extension of this method can also be used to discover new geometric theorems. That is, we can find out complementary conditions such that the geometric statement becomes true or true on components. Some illustrative examples will be presented to show how the method works.

This is joint work with Deepak Kapur, Yao Sun and Jie Zhou.

Keywords: Automatic Proving and Discovering, Geometric Theorem, Groebner Bases

[1]KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China
School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China

dwang@mmrc.iss.ac.cn

Sponsor Presentation

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

New features in Maple 2018

Daniel Skoog[1]

We will present an overview of new features in Maple 2018 including updates to the Maple interface such as the context panel, improved tools for writing Maple code, and options for protecting your content. We will also discuss improvements and additions in areas such as interpolation, calculations with units, date and time, thermochemical computations, computational geometry, symbolic integration, and discuss some applications.

[1]Maple Product Manager
Maple at Maplesoft
Waterloo, Ontario, Canada

S1
General Session

This session is for talks that do not fit into any of the other ACA sessions. All proposals in the scope of the conference are welcome.

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Randomized Algorithms for Normal Basis in Characteristic Zero

Mark Giesbrecht[1], **Armin Jamshidpey**[1], **Éric Schost**[1]

For a finite Galois extension K/F with $G = \mathrm{Gal}(K/F)$, there exists an element $\alpha \in K$ such that its conjugates form an F-basis of K (as a vector space)[4, Theorem 6.13.1]. Having such a basis, which is known as normal basis, is useful for certain computational purposes.

There are efficient algorithms for constructing a normal basis in positive characteristics. For a deterministic algorithm see [1] and for randomized algorithms see [6] and [3]. In characteristic zero, deterministic algorithms are introduced in [2] and [5](for abelian extensions).

Our aim is to introduce randomized algorithms for constructing a normal basis in characteristic zero. We will present an algorithm for cyclic extensions and more generally abelian extensions. We also give a solution for Galois extensions with dihedral group as Galois group.

Keywords: Normal Basis, Cyclic Extension, Abelian Extension

References

[1] DANIEL AUGOT; PAUL CAMION, *Forme de Frobenius et vecteurs cycliques*. *C. R. Acad. Sci. Paris Sér. I Math.*, 318(2):183–188, 1994.

[2] KURT GIRSTMAIR, *An algorithm for the construction of a normal basis*. *J. Number Theory*, 78(1):36–45, 1999.

[3] ERICH KALTOFEN; VICTOR SHOUP. *Subquadratic-time factoring of polynomials over finite fields*. *Math. Comp.*, 67(223):1179–1197, 1998.

[4] SERGE LANG, *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[5] ALAIN POLI, *A deterministic construction for normal bases of abelian extensions*. *Comm. Algebra*, 22(12):4751–4757, 1994.

[6] JOACHIM VON ZUR GATHEN; MARK GIESBRECHT, *Constructing normal bases in finite fields*. *J. Symbolic Comput.*, 10(6):547–570, 1990.

[1]David R. Cheriton School of Computer Science
University of Waterloo
200 University Avenue West Waterloo, ON, Canada N2L 3G1
mwg@uwaterloo.ca
armin.jamshidpey@uwaterloo.ca
eschost@uwaterloo.ca

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Computer Algebra and Computer Science

Gereon Kremer[1]

Certain fields within computer science commonly make use of methods from computer algebra. A prominent example for that is satisfiability modulo theories (SMT) solving that extends the traditional question of satisfiability of propositional logic formulas to first-order theories. We consider nonlinear real problems in particular which produces a need for methods to deal with nonlinear real constraints.

This topic is also an important topic in computer algebra, a community that deals with very similar questions but is surprisingly disjoint from the SMT solving community. The disjointness of these groups used to be a significant obstacle for any transfer of knowledge. The SC^2 project tries to resolve this hurdle by forging new collaborations between the communities of satisfiability checking and symbolic computation.

We present SMT solving as an application of methods from computer algebra and motivate functional requirements and use cases for these methods that are uncommon but very important for SMT solving. Though we can modify existing methods to a certain degree, we as computer scientists depend on the computer algebra community to solve some issues. We show several projects that yielded successful adaptations of methods like Gröbner bases [2], virtual substitution [1] or cylindrical algebraic decomposition [3] to our applications.

Finally we give examples of existing implementations of methods from computer algebra CoCoALib and Maple – that we struggled to integrate in a meaningful way. We provide insights into the actual problems and hope to suggest new directions of research that ease the cooperation between computer science and computer algebra in the future.

Keywords: Computer Algebra, Computer Science, Satisfiability Modulo Theories Solving, Gröbner Bases, Cylindrical Algebraic Decomposition, Virtual Substitution

References

[1] Florian Corzilius and Erika Abraham. Virtual Substitution for SMT Solving. In *FCT'11*, volume 6914 of *LNCS*, pages 360–371. Springer, 2011.

[2] Sebastian Junges, Ulrich Loup, Florian Corzilius, and Erika Abraham. On Gröbner Bases in the Context of Satisfiability-Modulo-Theories Solving over the Real Numbers. In *CAI'13*, volume 8080 of *LNCS*, pages 186–198. Springer, 2013.

[3] Gereon Kremer, Florian Corzilius, and Erika Abraham. A Generalised Branch-and-Bound Approach and its Application in SAT Modulo Nonlinear Integer Arithmetic. In *CASC'16*, volume 9890 of *LNCS*, pages 315–335. Springer, 2016.

[1]Theory of Hybrid Systems
RWTH Aachen University
52056 Aachen Germany
gereon.kremer@cs.rwth-aachen.de

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Conversion of element representations in Galois rings

Juan Carlos Ku-Cauich[1], **Guillermo Morales-Luna**[2]

A Galois ring is a finite ring with unity such that the divisors of zero, together with zero itself, form a principal ideal, generated by an element of the form pe, where e is the ring unit and p is a prime number. For any prime p and two integers s, m, the map

$$\pi_p : \mathbb{Z}_{p^s}[X] \to \mathbb{F}_p[X]\ ,\ g(X) = \sum_{j=0}^{m-1} a_j X^j \mapsto g(X) \bmod p = \sum_{j=0}^{m-1} (a_j \bmod p) X^j,$$

is a ring homomorphism. An irreducible polynomial $h(X) \in \mathbb{Z}_{p^s}[X]$ is basic if $\pi_p(h(X))$ is irreducible in $\mathbb{F}_p[X]$ and in this case $\mathbb{Z}_{p^s}/\langle h(X)\rangle$ is a Galois ring, denoted $GR(p^s, m)$. Let $\eta = X + \langle h(X)\rangle \in GR(p^s, m)$, then $h(\eta) = 0$ and $\mathbb{F}_{p^m} \approx [\mathbb{Z}_p[X]/\langle \pi_p(h(X))\rangle]$. Hence, $GR(p^s, m) = \mathbb{Z}_{p^s}[\eta]$ and each element in the Galois ring can be written in an additive form: $\sum_{j=0}^{m-1} a_j \eta^j$, with $a_j \in \mathbb{Z}_{p^s}$.

A polynomial $g(X) \in \mathbb{Z}_{p^s}[X]$ is basic primitive if $\pi_p(g(X))$ is primitive in $\mathbb{F}_p[X]$. It is well known [4] that there is an element $\xi \in GR(p^s, m)$ and a basic primitive polynomial $g(X) \in \mathbb{Z}_{p^s}[X]$ of degree m such that $o(\xi) = p^m - 1$, $g(\xi) = 0$, $g(X)|(X^{p^m-1} - 1)$ in $\mathbb{Z}_{p^s}[X]$ and the following two properties hold:

- $GR(p^s, m) = \mathbb{Z}_{p^s}[\xi]$
- Each element in $GR(p^s, m)$ can be written uniquely in a p-adic form: $\sum_{k=0}^{s-1} b_k p^k$, with $b_k \in \mathcal{T}(g(X))$, where $\mathcal{T}(g(X)) = \{0\} \cup \left(\xi^i\right)_{i=0}^{p^m-2}$ is a Teichmüller set.

Each primitive polynomial in $\mathbb{F}_p[X]$ characterizes a set of basic primitive polynomials in $\mathbb{Z}_{p^s}[X]$, namely its inverse image under the projection π_p. The p-adic representation depends on the chosen basic primitive polynomial.

We have developed a series of programs, basically in `sage`, to find monic basic primitive polynomials and convert additive representations into p-adic representations of the Galois ring elements, and conversely.

For any $m \in \mathbb{Z}^+$ there is [2] a monic primitive polynomial $f_{pm}(X) \in \mathbb{F}_p[X]$ dividing $P_{pm}(X) = X^{p^m-1} - 1$ in $\mathbb{F}_p[X]$. Then, by Hensel Lift [3] there is a monic basic primitive polynomial $f_{psm}(X) \in \mathbb{Z}_{p^s}[X]$ dividing $P_{pm}(X)$ in $\mathbb{Z}_{p^s}[X]$ with projection $f_{pm}(X)$. Since $f_{pm}(X) \in \mathbb{F}_p[X]$ is irreducible with no multiple roots, the polynomial $f_{psm}(X) \in \mathbb{Z}_{p^s}[X]$ is unique [4]. Hence, a natural correspondence $f_{pm}(X) \leftrightarrow f_{psm}(X)$ arises, and in most cases it is not the identity, namely $f_{pm}(X) \neq f_{psm}(X)$ in $\mathbb{Z}_{p^s}[X]$.

In the worst case, for small values of m and s the search of the Hensel lift polynomial $f_{psm}(X) \in \mathbb{Z}_{p^s}[X]$ can be done exhaustively. Alternatively, a list [2] of monic primitive polynomials in the ring $\mathbb{F}_p[X]$ may be provided in order to consider the inverse images of those polynomials under the projection modulus p.

The interest in finding effective and efficient representation conversions is due to the implementation of authentication codes based on the Gray transform [1].

Keywords: Galois rings, Teichmüller elements, symbolic computation

References

[1] JUAN CARLOS KU-CAUICH AND HORACIO TAPIA-RECILLAS, Systematic authentication codes based on a class of bent functions and the Gray map on a Galois ring. *SIAM J. Discrete Math.*, **27**(2), 1159–1170 (2013).

[2] RUDOLF LIDL AND HARALD NIEDERREITER, *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2 edition, 1996.

[3] B. R. MCDONALD, *Finite Rings with Identity*. Pure and Applied Mathematics Series. Marcel Dekker Incorporated, 1974.

[4] Z.-X. WAN, *Lectures on Finite Fields and Galois Rings*. World Scientific, Singapore, 2003.

[1]Computer Science
CINVESTAV-IPN
Mexico City, Mexico
jckc35@hotmail.com

[2]Computer Science
CINVESTAV-IPN
Mexico City, Mexico
gmorales@cs.cinvestav.mx

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Automatic generation of diagrammatic subway maps for any date with Maple

Alberto Almech[1], **Eugenio Roanes-Lozano**[2]

The second author was one of the authors of a computer package written in Maple that could automatically generate railway maps of a network for any date. This package was presented at ACA'2008 and its design and implementation is described in [1]. Each section of the network was coloured accordingly to its characteristics (single / double track, electrified / non electrified, opened / closed / greenway,...). The position of the nodes (stations, junctions,...) was obtained from a list of geographical coordinates.

The work presented here deals with a similar although not identical case: subway networks are treated as graphs with the help of a computer algebra system in order to obtain the diagrammatic map for any date.

Most metro network plans follow more or less closely the ideas introduced by Harry Beck in his diagrammatic design of London subway map (the distances between stations and geographic orientation of the lines don't have to be respected, as the clarity and the number of stations between two stations is the key information to be visualized).

Therefore allocating nodes is far simpler, and we have decided to manually allocate the stations on a predefined grid.

The situation is also simpler because all lines are double track and electrified. For instance in Madrid subway there are minor differences between lines, such as the kind of catenary (classic or rigid), the gauge (narrow / broad),... that will not be considered here. Each node and edge of the graph has dates associated: inauguration date / closure date –the latter if applies.

The package takes advantage of the simplifications w.r.t. [1] mentioned above and the features of *Maple's Networks* package. This way the approach, although general, can be implemented in relatively few lines of code.

We know of no other similar works.

The work is illustrated with the case of Madrid subway network, one of the biggest ones in the world.

Keywords: Graph theory, Network models, Diagrammatic maps, Subways

References

[1] E. ROANES-LOZANO, A. MARTÍNEZ-ZARZUELO, A. GARCÍA-ÁLVAREZ, M. J. WESTER, E. ROANES-MACÍAS Automatically Obtaining Railway Maps from a Set of Historical Events *RACSAM (Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales, Serie A, Matemáticas)* **105**(1), 149–165 (2011). DOI 10.1007/s13398-011-0010-1

[1]Facultad de CC. Matemáticas, Universidad Complutense de Madrid
Plaza de Ciencias s/n, 28040-Madrid, Spain
albermech@gmail.com

[2]Instituto de Matemática Interdisciplinar &
Depto. de Álgebra, Geometría y Topología
Facultad de Educación, Universidad Complutense de Madrid
c/ Rector Royo Villanova s/n, 28040-Madrid, Spain
eroanes@mat.ucm.es

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Detecting truth, just on parts, in automated reasoning in geometry*

Zoltán Kovács[1], **Tomás Recio**[2] and **M. Pilar Vélez**[3]

We introduce and discuss, through a computational algebraic geometry approach, the automatic reasoning handling of propositions that are simultaneously true and false over some relevant collections of instances. A rigorous, algorithmic criterion is presented for detecting such cases, and its performance is exemplified through the implementation of this test on the dynamic geometry program *GeoGebra*.

The algebraic geometry approach to automated reasoning in geometry proceeds by translating a geometric statement $\{H \Rightarrow T\}$ into polynomial expressions, after adopting a coordinate system. Then, the geometric instances verifying the hypotheses can be represented as the solution of a system of polynomial equations $V(H) = \{h_1 = 0, \ldots, h_r = 0\}$ (*hypotheses variety*) they are represented algebraically by the ideal (of hypotheses) $H = \langle h_1 = 0, \ldots, h_r = 0\rangle$ generated by such polynomials. Analogously, the thesis is represented as the solution of a polynomial $V(T) = \{f = 0\}$, describing the hypotheses (resp. the thesis) variety.

Thus, when $V(H) \subseteq V(T)$ we can say that the theorem is *always true*. But this fact rarely happens, even for well established theorems, because the algebraic translation of the geometric construction described by the hypotheses usually forgets explicitly excluding some degenerate cases, cf. [4].

Thus, a delicate, but more useful, approach for automated reasoning consists in exhibiting, first, a collection of independent variables modulo H, so that no polynomial relation among them holds over the whole $V(H)$ (*independent variables modulo* H). Now, the irreducible components of $V(H)$ where these variables do remain independent are assumed to describe *non-degenerate* instances.

Accordingly, a statement is called *generally true* if the thesis holds, at least, over all the non-degenerate components. On the other hand, if over each non-degenerate component the thesis does not identically vanish, the statement is labeled as *generally false*. Remark that this last includes the *always false* case, where the thesis does not hold at all. A more detailed description of this quite established terminology (with small variants) can be consulted, for instance, at [6], [3] or [7]. It follows from the definition that to be generally true and to be generally false are incompatible.

However—and this is the object of interest in this talk—there are statements which happen to be, simultaneously, not generally true and not generally false, i.e. statements that are *true, just on some components*. Recently, in [7], a new terminology

*Partially supported by the Spanish Research Project MTM2017-88796-P Computación simbólica: nuevos retos en álgebra y geometría y sus aplicaciones

to describe such cases has been introduced, labelling as *generally true on components* or, simply, as *true on components*; moreover [7] presents an algorithmic test to check this property. We have decided—for the better comprehension of this notion by general users of dynamic geometry programs implementing this feature, such as *GeoGebra*—to label such statements in a more colloquial way, as statements *true on parts, false on parts*, in some specific sense we will describe in detail below.

Let us first start analyzing a simple example. Consider points $A(0,0), B(2,0)$ in the plane and construct circles $c = (x-0)^2 + (y-0)^2 - 3$ and $d = (x-2)^2 + (y-0)^2 - 3$, i.e. circle c is centered at A and circle d is centered at B and both have the same radius $r = \sqrt{3}$. Finally, we consider the two points of intersection of these circles, namely, $E(u,v)$ and $F(m,n)$. Thus, the hypotheses ideal is $\left\langle u^2+v^2-3, (u-2)^2+v^2-3, m^2+n^2-3, (m-2)^2+n^2-3 \right\rangle$.

The thesis states the parallelism of the lines AE and BF, that is, the vanishing of the polynomial $u \cdot n - v \cdot (m-2)$. The ideal of hypotheses is clearly zero-dimensional, so there are no independent variables, nor degenerate components. Its primary components, over the rationals, are

$$\left\langle v-n, (m-2)^2+n^2-3, (u-2)^2+v^2-3, m^2+n^2-3, u^2+v^2-3 \right\rangle$$
$$\left\langle v+n, (m-2)^2+n^2-3, (u-2)^2+v^2-3, m^2+n^2-3, u^2+v^2-3 \right\rangle.$$

It easy to check that the thesis is false over the first one and true over the second. This a clear, simple example of a neither true nor false, i.e. of a *true on components*, statement arising in an elementary geometry context (see other, less artificial examples in [6, 1]).

Obviously, since the idea of *true on components*, or *true on parts, false on parts*, is based on the concepts of degeneracy and of irreducible component, it follows that both the choice of the field over which the prime decomposition is performed (for example, the ideal H of the previous example has four components instead, if $\mathbb{Q}(\sqrt{2})$ is considered as base field) and the choice of the independent variables –which determine which components are to be considered as degenerate– could be essential.

About this last issue we would like to remark that when dealing with geometric statements it seems logical to take as independent variables the coordinates of the free points in the geometric construction we are dealing with; and we expect that its cardinality is the dimension of the hypotheses ideal. In most cases this "intuitively" maximal set of independent variables is maximum-size, but there are examples in which the coordinates of the free points in the geometric construction do not provide a maximum-size set of independent variables. See, for instance, Example 7 in [4], concerning Euler's formula regarding the radii of the inner and outer circles of a triangle with vertices $(-1,0), (1,0), (u[1], u[2])$. Here the dimension of the hypotheses variety is expected to be 2 (referring to the two coordinates of the only free vertex of the triangle), but applying the algebraic definition of independence it turns out to be three…, unless it is explicitly required, and added as a new hypothesis, that $(u[1], u[2])$ does not lie in the x-axis! This is a quite common problem—

related, as mentioned above, to the difficult *a priori* control and detail of all geometric degeneracies—and is already considered in the basic reference of [2].

The aim of this talk is to justify the specific interest of statements that, according to our terminology, are simultaneously *true on parts, false on parts* statements in the context of automated reasoning in geometry, pointing out the subtle, involved, issues deriving from the quirky algebraic behavior described in some of the examples above, as well as exhibiting a new, simpler way, of testing if a statement is true and false on parts, by just detecting if a pair of elimination ideals are zero or not. This test has been implemented in the dynamic geometry software GeoGebra and some illustrative examples can be found in `https://www.geogebra.org/m/zpDq7taB`.

This extended abstract is based on a recent work by the authors [5].

Keywords: geometry theorem proving and discovery, elementary geometry, Gröbner basis, elimination, true on components, GeoGebra

References

[1] F. BOTANA AND T. RECIO, On the unavoidable uncertainty of truth in dynamic geometry proving, *Mathematics in Computer Science* **10** (1), 5-25 (2016).

[2] S.C. CHOU, *Mechanical geometry theorem proving*, Mathematics and its Applications (41), D. Reidel Publishing Co., Dordrecht (1988).

[3] D.A. COX, J. LITTLE AND D. O'SHEA, *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra*, 4th revised ed. Undergraduate Texts in Mathematics, Springer International Publishing, Switzerland (2015).

[4] G. DALZOTTO AND T. RECIO, On protocols for the automated discovery of theorems in elementary geometry, *Journal of Automated Reasoning* **43**, 203-236 (2009).

[5] Z. KOVÁCS, T. RECIO AND M.P. VÉLEZ, *Detecting truth, just on parts*, Preprint: arXiv: 1802.05875 [cs.AI] (2018).

[6] T. RECIO AND M.P. VÉLEZ, Automatic discovery of theorems in elementary geometry, *Journal of Automated Reasoning* **23**, 3-82 (1999).

[7] J. ZHOU, D. WANG AND Y. SUN, Automated reducible geometric theorem proving and discovery by Gröbner basis method, *Journal of Automated Reasoning* **59** (3), 331-344 (2017).

[1]Private Pädagogische Hochschule der Diözese Linz
Salesianumweg 3, 4020 Linz
zoltan@geogebra.org

[2]Universidad de Cantabria
Avda. de los Castros, s/n, 39005 Santander (Spain)
tomas.recio@unican.es

[3]Universidad Antonio de Nebrija
C/ Pirineos, 55, 28040 Madrid (Spain)
pvelez@nebrija.es

S2
Computer Algebra Modeling in Science and Engineering

The progressive impact of the Computer Algebra Systems (CAS) in science-based disciplines vividly is noticeable. It is rare to encounter a scientific investigation that is immune from its beneficial influences. Symbolic capabilities of the CAS provides forum to perform amazing calculations that practically are impossible otherwise. Within the last 25 years, applications of the CAS are extended beyond the peculiarities of scientific disciplines such as: biology, chemistry, microbiology, and physics, and has become the tool of the choice for analyzing engineering and mathematical challenging problems. For instance, dynamic simulations of engineering issues are addressed and mathematical conjectures are formulated and verified. Applications of the CAS lend it beyond the researchers' tools and have become powerful pedagogical instruments. The latter is suitable to engage the computer savvy generation promoting the discipline of interest.

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

- Symbolic and numerical methods solving ODEs
- Modeling and simulation in physics
- Simulation of quantum computation
- Perturbation theories
- Stability and motion control
- Applications in biology, chemistry, and microbiology
- Modeling in finance and economics

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

To analysis of the tunneling effect through Schwarzschild barrier for spin 1/2 particles

A. V. Chichurin[1], **E. M. Ovsiyuk**[2], **V. M. Red'kov**[3]

For massless Dirac particle, the general mathematical and numerical study of the particle tunneling process through effective potential barrier generated by Schwarzschild black hole background is done. The study will be based on the use of 8 Frobenius solutions of related 2-nd order differential equations with nonregular singularities of the rank 2. We construct these solutions in explicit form and prove that power series involved in them are converged in all physical regions of the physical region of the variable $r \in (1, +\infty)$. Results for tunneling effect significantly differ for two situations: one when the particle falls on the barrier from within and another when the particle falls from outside. The main novelty of the study consists in the use of 8 Frobenius solutions. Mathematical structure of the derived asymptotic relations is exact, however analytical expressions for involved convergent powers series are not known, and further study is based on numerical summing the series.

Keywords: Dirac particle, Schwarzschild field, tunneling process, Frobenius solutions, reflection coefficient

References

[1] CHICHURIN A.V., OVSIYUK E. M., RED'KOV V.M., *Modeling the quantum tunneling effect for a particle with intrinsic structure in presence of external magnetic field in the Lobachevsky space*. Computers and Mathematics with Applications 75 (2018) 1550–1565

[2] REDKOV V.M., OVSIYUK E.M., *Quantum Mechanics in Space of Constant Curvature*. Nova Science Publishers, New York, 2012.

[3] OVSIYUK E.M., CHICHURIN A.V., RED'KOV V.M., *Nonrelativistic vector particle in Coulomb field on the background of Lobachevsky geometry: analytical and numerical study, visualization*. Stud. I Mater. Eur. Univ. Warsaw 10 (2015) 45–57.

[1]Institute of Mathematics and Computer Science
The John Paul II Catholic University of Lublin
Lublin, 20-708, Poland
achichurin@gmail.com

[2]Physics and Mathematics Department
Mozyr State Pedagogical University named after I.P. Shamyakin
28 Studencheskaya Str, Mozyr 247760, BELARUS
e.ovsiyuk@mail.ru

[3]Laboratory of Theoretical Physics
B. I. Stepanov Institute of Physics of NAS of Belarus
v.redkov@ifanbel.bas-net.by

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Numerical study of multiphase flow and viscous fingering in a heterogeneous porous medium

Hassane DJEBOURI[1], **Salah ZOUAOUI**[1], **Kamal MOHAMMEDI**[2] and **Ali BILEK**[1]

This work deals with the numerical study of an immiscible water-oil displacement through a porous medium. This type of flow finds its application in many industrial processes [1]. The purpose of this work is to see the effect of the heterogeneity of the porous medium on the instability of the interface of the two fluids. This instability develops by the formation of viscous fingering at the interface [2].
The first work on this phenomenon began in the fifties (1951), but it still remains a topic of interest for many researchers [2]. In order to investigate the effect of the heterogeneity of the medium on this phenomenon, four cases are considered: the first one is a reference case where the porous medium is homogeneous. For the second and the third case, the medium is composed of two zones of the same porosity but of different permeability. The ratio of permeability between the two zones is equal to 1/3. In the second case, the injection is made in the zone that has the higher permeability and inversely in the third case.
In the last case we are interested in a fractured porous medium. The fracture has an opening of 2cm located in the middle of the domain (see figure 1).

Mathematical model

The studied domain is two-dimensional $\Omega \in R^2$. The mass conservation equations supplemented by Darcy's law allows to write [3]:

$$\frac{\partial(\phi.\rho_i.S_i)}{\partial t} - \nabla.\left(\rho_i \frac{\mathrm{K}.K_{ri}}{\mu_i}(\nabla P_i)\right) = 0 \qquad i = oil, water \tag{1}$$

Where ϕ and K are respectively the porosity and the permeability of the porous medium. K_{ri}, S_i, ρ_i and μ_i are respectively the relative permeability, the saturation, the density and the viscosity of the i phase.
This system of equations is completed by the following relations:

$$S_o - S_w = 1 \tag{2}$$

$$K_{ri} = K_{ri}(S_{ri}) \tag{3}$$

$$P_c = P_o - P_w \tag{4}$$

The Corey and CSF (Continuum Surface Force) models are used to calculate relative permeability and capillary pressure, respectively.
The initial conditions as well as the boundary conditions are:

- At $t = 0$, the medium is completely saturated with oil then: $S_o = 1$.
- The boundaries of the domain are impervious: $\frac{\partial S_i}{\partial n} = 0$ et $\frac{\partial P_i}{\partial n} = 0$.
- Injection and production point pressures are $1.79MPa$ and $1.31MPa$.

Figure 1: Different porous media studied

Table 1: Physical properties of porous media

	midium1	midium2		midium3		midium4	
Porosity (%)	30	Zone1	Zone2	Zone1	Zone2	Zone1	Zone2
		30	30	30	30	30	30
Absolute Permébility (m^2)	$130x10^{-12}$	$130x10^{-12}$	$43.33x10^{-12}$	$43.33x10^{-12}$	$43.33x10^{-12}$	$130x10^{-12}$	$130x10^{-12}$

Résultats

The finite volume method is used to solve this problem. Some results are presented:

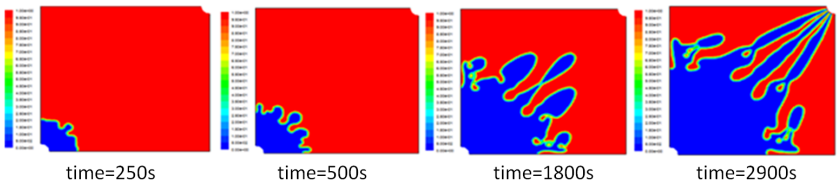


Figure 2: Displacement fronts and fingering patterns for medium1 at different times

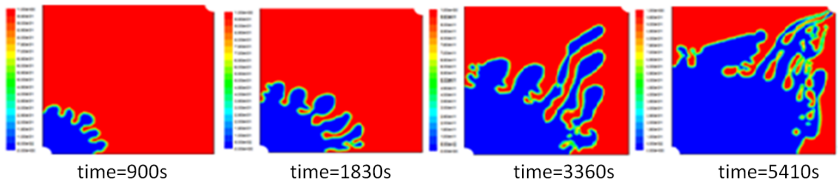


Figure 3: Displacement fronts and fingering patterns for medium2 at different times

The following observations are made:

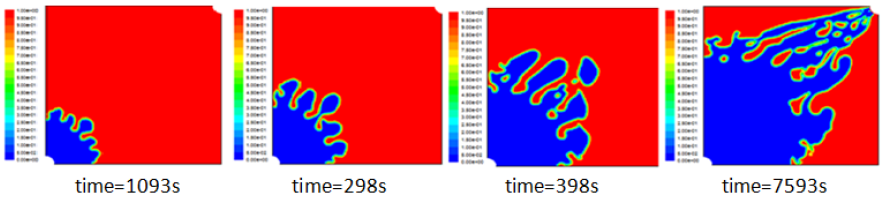


Figure 4: Displacement fronts and fingering patterns for medium3 at different times

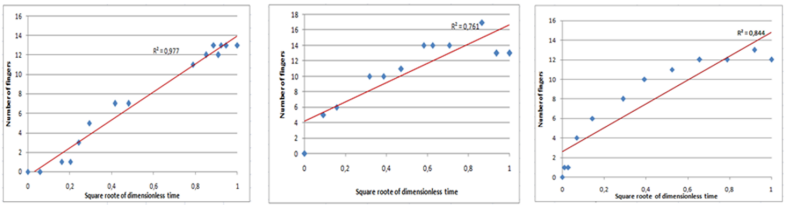


Figure 5: Number of fingers formed as a function of the square root of the dimensionless time for media 1, 2 and 3

- The characteristics of the porous medium modify the behavior of the water-oil interface and the appearance of breakthrough. This result is in agreement with previous studies.
- Viscous fingers tend to develop almost linearly according to the square root of time. These observations are in contradiction with the results of (Milad Arabloo et al, 2015) but in good agreement with the experimental results of de (Yadali Jamaloei et al, 2010) and (Shokrollahi et al, 2013).

Keywords: heterogeneous porous media, multiphase flow, viscous fingering, fracture

References

[1] MILAD ARABLOO ET AL., Characterization of viscous fingering during displacements of low tension natural surfactant in fractured multi-layered heavy oil systems. *Chemical Engineering Research and Design* **96**, 23–34 (2015).

[2] R. FARAJZADEH ET AL., Simulation of instabilities and fingering in surfactant alternating gas (SAG) foam enhanced oil recovery. *Journal of Natural Gas Science and Engineering, JNGSE* **34**, 1191–1204 (2016).

[3] T. SHEORY ET AL., Numerical experiments in the simulation of enhanced oil recovery. *Internat.J. Thermal Sci.* **40**(11), 981–997 (2001).

[1]LMSE Laboratory, Mechanical Engineering Department
Mouloud Mammeri University of Tizi-Ouzou
P.O. Box17 RP, 15000 Tizi Ouzou, Algeria
zouaoui_salah2003@yahoo.fr; zouaouisalah@ummto.dz

[2]Unité de Recherche Matériaux, Procédés et Environnement (URMPE)
MESOnexusteam
Université M'hamed Bougara Boumerdès
Algérie 35000
mohammedik@yahoo.com

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Leap-Frog Algorithm for interpolating reduced sparse data

Ryszard Kozera[1,2,3], **Lyle Noakes**[3]

We discuss the problem of fitting *ordered data points* $\mathcal{M} = \{x_i\}_{i=0}^n$ (with $n \geq 2$) from arbitrary Euclidean space E^m. The class $\mathcal{I}_T$ of piecewise C^2 interpolants $\gamma : [0,T] \rightarrow E^m$ (where $0 < T < \infty$) to interpolate reduced data $\mathcal{M}$ admits *free knots* $\mathcal{T} = \{t_i\}_{i=0}^n$ satisfying $\gamma(t_i) = x_i$ (here $t_0 = 0$ and $t_n = T$ are fixed). More precisely, it is assumed here that any choice of ordered interpolation knots $\{t_i\}_{i=0}^n$ together with $\mathcal{M}$ generates a curve $\gamma \in C^1([0,T])$ which is also C^2 over each subsegment (t_i, t_{i+1}) (where $i = 0, 1, \ldots, n-1$). A standard result (see [1] or [2]) claims that for given fixed knots $\{t_i\}_{i=0}^n$ the *optimal* curve $\gamma_{opt} \in \mathcal{I}_T$ to minimize:

$$\mathcal{J}_T(\gamma) = \sum_{i=0}^{n-1} \int_{t_i}^{t_{i+1}} \|\ddot{\gamma}(t)\|^2 dt \ , \tag{1}$$

coincides with the unique natural cubic spline $\gamma_{opt} = \gamma_{NS}$. Thus upon relaxing the unknown knots $\{t_i\}_{i=1}^{n-1}$, optimizing (1) over $\mathcal{I}_T$ reduces into a respective search over the class of natural splines, clearly contained in $\mathcal{I}_T$. Consequently, as each γ_{NS} is uniquely determined by data points $\mathcal{M}$ and the respective knots $\mathcal{T}$ (see [1]) the above infinite dimensional optimization task forms a finite dimensional one. Indeed, as recently shown (see [3]) for given $\mathcal{M}$, the task of minimizing (1) over $\mathcal{I}_T$ reformulates into optimizing the corresponding J_0 this time depending merely on $(t_1, t_2, \ldots, t_{n-1})$ variables, subject to $t_0 = 0 < t_1 < \ldots < t_n = T$. The latter constitutes a highly non-linear optimization task depending on $n-2$ variables. The application of standard numerical schemes to optimize J_0 often results in computational difficulties. In this work we adapt *a Leap-Frog scheme* (see e.g. [4]) to numerically optimize J_0. In our setting, this iterative scheme relies on the overlapped local optimizations each time depending on one variable only. The symbolic calculations performed with the aid of *Mathematica* software package (see e.g. [5]) permit to derive the corresponding local optimization schemes and to address the unimodality issue. Finally, the numerical tests comparing Leap-Frog scheme against Newton's or Secant methods are also carried out.

Keywords: Interpolation, reduced data, optimization.

References

[1] C. DE BOOR, *A Practical Guide to Spline*. Springer-Verlag, New York Heidelberg Berlin, 1985.

[2] B.I. KVASOV, *Methods of Shape-Preserving Spline Approximation*. World Scientific Publishing Company, Singapore, 2000.

[3] R. KOZERA; L. NOAKES, Non-linearity and non-convexity in optimal knots selection for sparse reduced data. *Computer Algebra in Scientific Computing*, *Lecture Notes in Computer Science*, Springer, **10490**, 257–271 (2017).

[4] R. KOZERA; L. NOAKES, Nonlinearities and noise reduction in 3-source photometric stereo. *Journal of Mathematical Imaging and Vision* **18**(2), 119–127 (2003).

[5] S. WOLFRAM, *The Mathematica Book*. Wolfram Media, 2003.

[1]Faculty of Applied Informatics and Mathematics
Warsaw University of Life Sciences - SGGW
Nowoursynowska str. 159, 02-776 Warsaw, Poland
ryszard.kozera@gmail.com

[2]Faculty of Mathematics, Informatics and Landscape Architecture
The John Paul II Catholic University of Lublin
Konstantynów str. 1 H, 20-708 Lublin, Poland

[3]School of Computer Science and Software Engineering
The University of Western Australia
Stirling Highway 35, Crawley, Perth, WA 6009, Australia

[4]School of Mathematics and Statistics
The University of Western Australia
Stirling Highway 35, Crawley, Perth, WA 6009, Australia
lyle.noakes@uwa.edu.au

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Reparameterization and piecewise cubics for interpolating reduced data

Ryszard Kozera[1,2,3], **Magdalena Wilkołazka**[3]

We discuss the problem of estimating the unknown 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 $Q_m = \{q_i\}_{i=0}^m$ in arbitrary Euclidean space E^n satisfying $q_i = \gamma(t_i)$. Here the respective knots $\mathcal{T}_m = \{t_i\}_{i=0}^m$ fulfilling $t_i < t_{i+1}$ are not given. In order to fit Q_m with any interpolation scheme (see e.g. [1]), the missing knots $\mathcal{T}_m$ must be replaced somehow with $\hat{\mathcal{T}}_m = \{\hat{t}_i\}_{i=0}^m$ subject to $\hat{t}_i < \hat{t}_{i+1}$. One of the possible choices is the so-called *exponential parameterization* depending on a single parameter $\lambda \in [0,1]$ and Q_m - see e.g. [2]. Note that $\lambda = 1$ renders a well-know *cumulative chord parameteriztion*. Different interpolation schemes are studied to fit reduced data Q_m - see e.g. [3], [4] or [5].

Recent work [6] and [7] addresses the issue of interpolating Q_m based on exponential parameterization applied to either modified Hermite interpolants $\hat{\gamma}_H \in C^1$ or to piecewise C^1 Lagrange cubics $\hat{\gamma}_C$. It is proved that for $\hat{\gamma} = \gamma_H$ or $\hat{\gamma} = \hat{\gamma}_C$ the following asymptotics in $\gamma \in C^4$ estimation holds (uniformly over $[0,T]$):

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

Here the mapping $\psi : [0,T] \to [0,\hat{T}]$ for each $\hat{\gamma}$ is specifically constructed. In this work we formulate and prove (with the aid of *Mathematica* package [8]) sufficient conditions for ψ to be a genuine reparameterization. Geometrical and algebraic insight is also given. Finally, with the aid of symbolic and analytic calculation sharpness of (1) is verified and justified.

Keywords: Interpolation, reduced data, convergence, sharpness and parameterization.

References

[1] C. DE BOOR, *A Practical Guide to Spline*. Springer-Verlag, New York Heidelberg Berlin, 1985.

[2] B.I. KVASOV, *Methods of Shape-Preserving Spline Approximation*. World Scientific Publishing Company, Singapore, 2000.

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

[4] R. KOZERA; L. NOAKES, Piecewise-quadratics and ε-uniformly sampled reduced data. *Applied Mathematics and Information Sciences* **10**(1), 33–48 (2016).

[5] R. KOZERA; L. NOAKES, C^1 interpolation with cumulative chord cubics. *Fundamenta Informaticae* **61**(3-4), 285–301 (2004).

[6] R. KOZERA; M. WILKOŁAZKA, Convergence order in trajectory estimation by piecewise-cubic and exponential parameterization. *Mathematical Modelling and Analysis*, submitted.

[7] R. KOZERA; M. WILKOŁAZKA, Modified Hermite interpolation with exponential parameterization. *Mathematics in Computer Science*, submitted.

[8] S. WOLFRAM, *The Mathematica Book*. Wolfram Media, 2003.

[1]Faculty of Applied Informatics and Mathematics
Warsaw University of Life Sciences - SGGW
Nowoursynowska str. 159, 02-776 Warsaw, Poland
ryszard.kozera@gmail.com

[2]School of Computer Science and Software Engineering
The University of Western Australia
Stirling Highway 35, Crawley, Perth, WA 6009, Australia

[3]Faculty of Mathematics, Informatics and Landscape Architecture
The John Paul II Catholic University of Lublin
Konstantynów str. 1 H, 20-708 Lublin, Poland
magda.wilkolazka@gmail.com

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Computing perturbations in two-planetary three-body problem with masses varying non-isotropically at different rates

Mukhtar Minglibayev[1,2], **Alexander Prokopenya**[3], **Saule Shomshekova**[1,2]

The classical problem of three bodies of variable masses is considered in the case when two of the bodies are protoplanets and the masses vary non-isotropically at different rates. Reactive forces appearing due to the change of masses complicate the problem substantially and general solution of the equations of motion cannot be found in symbolic form. So the problem is analyzed in the framework of the perturbation theory in terms of the osculating elements of aperiodic motion on quasi-conic sections [1, 2]. An algorithm for symbolic computation of the perturbing function and its expansions in terms of eccentricities and inclinations is discussed in detail.

Keywords: Three-body problem, protoplanets, variable masses, perturbations, Mathematica

References

[1] M.ZH. MINGLIBAYEV, *Dynamics of Gravitating Bodies of Variable Masses and Sizes*. Lambert Academic Publ., 2012.

[2] M.ZH. MINGLIBAYEV, A.N. PROKOPENYA, G.M. MAYEMEROVA, ZH.U. IMANOVA, Three-body problem with variable masses that change anisotropically at different rates. *Mathematics in Computer Science* **11**, 383–391 (2017).

[1]al-Farabi Kazakh National University
al-Farabi av. 71, 050040, Almaty, Kazakhstan
minglibayev@gmail.com

[2]Fesenkov Astrophysical Institute
Observatoriya 23, 050020, Almaty, Kazakhstan
shomshekova.saule@gmail.com

[3]Department of Applied Informatics
Warsaw University of Life Sciences – SGGW
Nowoursynowska 166, 02-787, Warsaw, Poland
alexander_prokopenya@sggw.pl

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Motion of two bodies coupled by a spring on a rough plane with variable coefficient of friction: simulation with Mathematica

Alexander N. Prokopenya[1]

Two bodies of the same mass m connected by a spring move along a straight line Ox of a horizontal plane which is smooth for $x < 0$ and is rough for $x \geq 0$. Initially both bodies are located in the domain $x < 0$ and have the same velocity $v_0 > 0$. Assume that at the initial instant of time $t = 0$ the spring is not deformed and the x-coordinates of the bodies are $x_1(0) = -l_0$, $x_2(0) = 0$, where l_0 is the length of non-deformed spring. The problem is to investigate the motion of the system when the second body enters the domain $x > 0$ and starts to move on a rough surface. In this case the second body is acted on by the dry friction force directed opposite to the velocity of the body (see [1, 2]). As the spring is compressed and exerts a force on each of the bodies, one can write the equations of motion in the form

$$\begin{aligned} \ddot{x}_2 &= -\mu g - \frac{k}{m}(x_2 - x_1 - l_0), \\ \ddot{x}_1 &= \frac{k}{m}(x_2 - x_1 - l_0), \end{aligned} \tag{1}$$

where μ is a friction factor, k is the spring constant, g is the gravity acceleration, and m is a mass of each body. It is assumed that only the second body moves on the rough semi-plane and its velocity $\dot{x}_2(t) > 0$. Solution to the system (1) can be found in symbolic form and application of the built-in Mathematica function *DSolve* (see [3]) gives

$$\begin{aligned} x_1(t) &= -l_0 + v_0 t - \frac{\mu g t^2}{4} + \frac{\mu m g}{4k}\left(1 - \cos\left(\sqrt{\frac{2k}{m}}t\right)\right), \\ x_2(t) &= v_0 t - \frac{\mu g t^2}{4} - \frac{\mu m g}{4k}\left(1 - \cos\left(\sqrt{\frac{2k}{m}}t\right)\right). \end{aligned} \tag{2}$$

Analysis of solution (2) shows that for some instant of time $t = t_1$ which is a root of the equation

$$v_0 - \frac{\mu g t_1}{2} = \frac{\mu g}{2}\sqrt{\frac{m}{2k}}\sin\left(\sqrt{\frac{2k}{m}}t_1\right), \tag{3}$$

velocity of the second body $\dot{x}_2(t_1)$ becomes equal to zero while $x_1(t_1) < 0$ and $\dot{x}_1(t_1) > 0$. If the condition $|x_2(t_1) - x_1(t_1) - l_0| < \mu m g/k$ is fulfilled the second body stops while the first one continues to move. Further motion of the system

depends on the parameters k, m, l_0, μ, v_0, and different scenarios may be realized. Doing necessary symbolic and numerical calculations, we show that if elastic properties of the spring are asymmetric and its constant for stretching is greater than its constant for compressing then there exist such values of the system parameters for which the bodies are reflected from the rough semi-plane. Investigation of this interesting phenomenon is a main aim of the present talk.

Keywords: Motion of coupled bodies, dry friction, simulation, Wolfram Mathematica

References

[1] BO N.J. PERSSON, *Sliding friction. Physical principles and applications*. Springer-Verlag, Berlin, Heidelberg, 2000.

[2] LE X. ANH, *Dynamics of mechanical systems with Coulomb friction*. Springer-Verlag, Berlin, Heidelberg, 2003.

[3] S. WOLFRAM, *An elementary introduction to the Wolfram Language*. Wolfram Media, Champaign, IL, USA, 2017.

[1]Department of Applied Informatics
Warsaw University of Life Sciences – SGGW
Nowoursynowska str. 166, 02-787 Warsaw, Poland
alexander_prokopenya@sggw.pl

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

A study of sensitivity of nonlinear oscillations of a CLD parallel circuit to parametrization of Esaki diode

Haiduke Sarafian[1]

Esaki diode, also known as, a tunneling diode [1] is a peculiar nonlinear electronic element possessing negative ohmic resistance. We consider a multi-mesh circuit composed of three elements: a charged capacitor (C), a self-inductor (L), and an Esaki diode (D). All three elements in the circuit are parallel. We parametrize the I-V characteristics of the diode and derive the circuit equation; this is a nonlinear differential equation. Applying a Computer Algebra System (CAS) specifically Mathematica [2] we solve the equation numerically conducive to a diode dependent parametric solution. The solution is oscillatory. In this note we investigate the sensitivity of the nonlinear oscillations as a function of these parameters. Particularly we establish the fact that for a set of parameters the tunneling diode becomes an ohmic resistor and the circuit equation simplifies to a classic CLR parallel circuit with linearly damped oscillations. Mathematica simulation assists visualizing the transition.

Keywords: Esaki Diode, Electrical Nonlinear Oscillations, Computer Algebra System, Mathematica

References

[1] *Leo Esaki diode*. https://en.wikipedia.org/wiki/Tunnel_diode

[2] *Mathematica^{TM} (2017) is symbolic computation software*, V11.2, Wolfram Research Inc.

[1]The Pennsylvania State University
University College
York, PA 17403
has2@psu.edu

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

3D Stress analysis of a loaded birefringent sphere by photoelastic experiment and finite elements method

Kamel Touahir[1], **Ali Bilek**[1], **Said Larbi**[1], **Said Djebali**[1] and **Philippe Bocher**[2]

This paper deals with a contact problem developed in a birefringent sphere loaded by a plan along its diameter. In mechanical systems, contacts between moving elements can give rise to high stresses that can cause damage. Several authors [1, 2, 3, 4, 5] have contributed to the understanding of contact problems. To improve the design and the durability, it is necessary to determine accurately the stress fields particularly in the neighborhood of the contact zones. The analyzed model consists of a birefringent deformable sphere loaded along its diameter by birefringent rigid plans. Stress fields are analyzed experimentally with plan polarized light and circularly polarized light; photoelastic fringes are used to calculate stresses. A finite elements analysis with Castem package allows calculating the stress fields. Comparison between the experimental solution and the finite element one shows good agreements.

Experimental analysis

The birefringent sphere is machined from a birefringent parallelepiped on a high speed numerically controlled machine. The model is then loaded inside an oven (figure 1left) at the stress freezing temperature (120^oC). A thermal cycle is used to freeze stresses within the volume of the model. The model is then mechanically sliced in a high speed rotating machine to prevent residual stresses. The birefringent

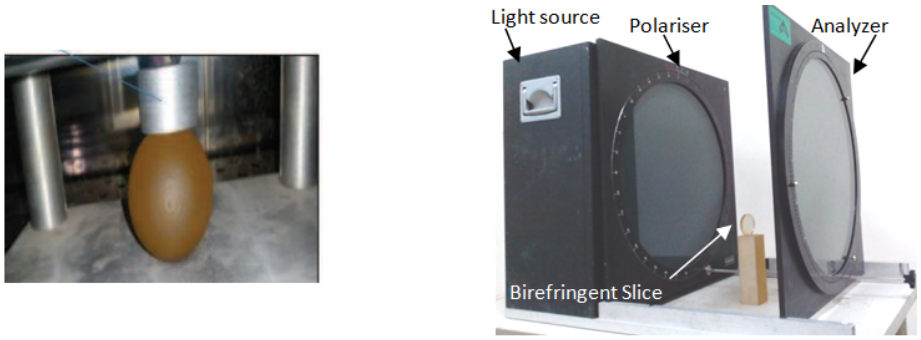


Figure 1: Sphere inside the oven (left), a slice analyzed in a polariscope (right)

slice is then positioned in the light path of a polariscope (figure 1 right) to obtain the photoelastic fringes. The light intensity after the analyzer is given by Eq. (1).

The terms $\sin^2 2\alpha$ and $\sin^2 \varphi/2$ give respectively the isoclinic fringe pattern and the isochromatic fringe pattern where α and φ are respectively the isoclinic parameter and the isochromatic parameter [6].

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

The experimental isochromatic fringes are used to determine the values of the principal stresses difference in the model by using the well known Eq. (2).

$$\sigma_1 - \sigma_2 = \frac{Nf}{e} \tag{2}$$

Where N is the fringe order, f is the photoelastic fringe value, and e is the model thickness. The values of the fringe order N are determined experimentally.
A $10mm$ thickness slice along the load direction (figure 2) is analyzed with plane polarized light on a regular polariscope. One can see clearly the isochromatics and the isoclinics developed on the model particularly in the neighborhood of the contact zones where stresses are higher (zone of maximum shear stress).

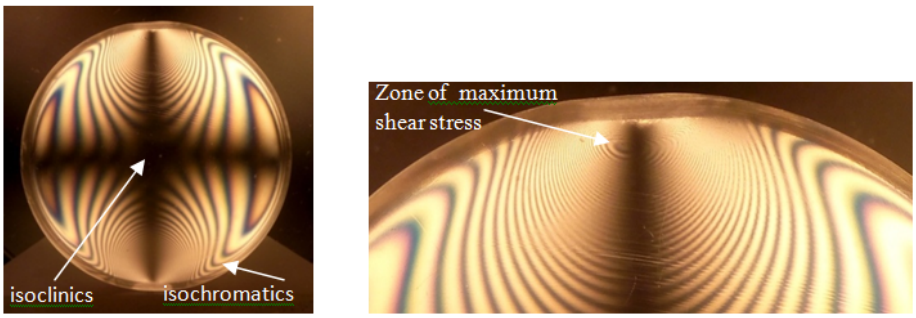


Figure 2: Photoelastic fringes obtained with plan polarized light

Numerical analysis

A finite element analysis is used to determine the stress fields developed in the models particularly in the neighborhood of the contact zones; a program developed under *castem package* allowed us to obtain stress values as well as numerical photoelastic fringes that can be compared to the experimental photoelastic fringes. The analysis is performed in the elastic domain. The meshing is refined in the neighborhood of the contact zone for a better simulation (figure 3).
The isoclinic fringe pattern is calculated with eq. (3) where α is the isoclinic parameter [6]. Once α is obtained the value of $\sin^2 2\alpha$ gives directly the isoclinic fringe pattern.

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

The simulated isochromatic fringe patterns are obtained with eq. (4). The different values of $\sin^2 \varphi/2$ give then easily the numerical isochromatic fringes.

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

The graph of variation of the principal stresses difference (Fig. 3) is obtained along the vertical axis. Stresses increase up to approximately $0.6MPa$ and then decrease as we move away from the contact zone. We can see relatively good agreement between the two solutions.

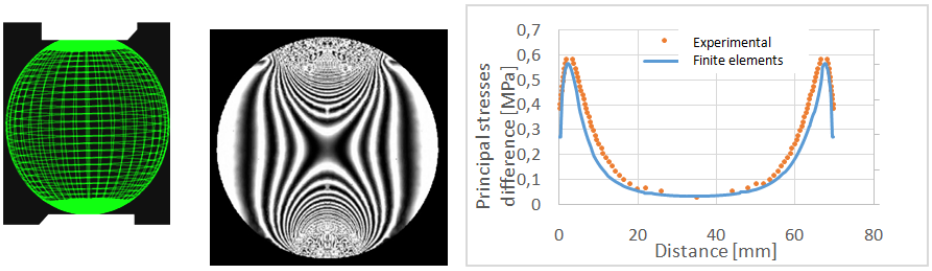


Figure 3: Model meshing and isochromatic fringes for a slice along the load direction

Keywords: photoelasticity, birefringent, isochromatic, isoclinic, contact, stress

References

[1] ABODOL RASOUL SOHOULI, ALI MAOZEMI GOUDARZI, REZA AKBARI ALASHTI, Finite Element Analysis of Elastic-Plastic Contact MechanicConsidering the Effect of Contact Geometry and Material Propertie. *Journal of Surface Engineered Materials and Advanced Technology* **1**(3), 125–129 (2011).

[2] J. A. GERMANEAU, F. PEYRUSEIGT, S. MISTOU, P. DOUMALIN AND J.C. DUPRÉ, Experimental study of stress repartition in aeronautical spherical plain bearing by 3D photoelasticity : validation of a numerical model. In *5th BSSM International Conference on Advances in Experimental Mechanics*, University of Manchester, UK,Sept. 2007.

[3] L. KOGUT & I. ETSION, Elastic-Plastic contact analysis of a sphere and a rigid flat. *Journal of Applied Mechanics* **69**(5), 657–662 (2002).

[4] BUDIMIR MIJOVICAND MUSTAPHA DZOCLO, Numerical contact of a Hertz contact between two elastic solids. *Engineering Modeling* **13**(3-4), 111–117 (2000).

[5] RABAH HACIANE, ALI BILEK, SAID LARBI, SAID DJEBALI, Photoelastic and numerical analysis of a sphere/plan contact problem. *Procedia Engineering* **114**, 277–182 (2015).

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

[1]LMSE Laboratory, Mechanical Engineering Department
Mouloud Mammeri University of Tizi-Ouzou
P.O. Box17 RP, 15000 Tizi Ouzou, Algeria
alibilek2000@yahoo.fr

[2]Mechanical Engineering Department
Ecole de Technologie Supérieure
1100 Rue Notre-Dame, Montreal, H3C 1K3, Canada

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Visualization of Planetary Motions Using KeTCindy

Satoshi Yamashita[1], **Kiyoshi Kitahara**[2], **Shuhei Miyake**[3], **Setsuo Takato**[4]

KeTCindy, a plug-in for a dynamic geometry software Cinderella, facilitates the creation of precise and beautiful drawings of 2D/3D graphics and their input into a LaTeX document. Moreover, KeTCindy can call other mathematical software to run a program and bring back the results. For a task of visualizing planetary motion, the authors call the computer algebra software Maxima to execute mathematical expression processing. Then they create PDF slides that portray planetary motion precisely based on the result[1].

About planetary motion, J. Kepler published the following three laws in 1619, having found them by analyzing the astronomical observations of T. Brahe.

1. The orbit of a planet is an ellipse with the Sun at one of the two focuses. Letting r be the distance from the Sun to the planet and letting θ be the angle to the planet's current position from its closest approach, as seen from the Sun, then the polar coordinates $(r,\ \theta)$ satisfy the polar equation of the ellipse:

$$r = \frac{l}{1 + \varepsilon \cos\theta}, \tag{1}$$

where l is the semi-latus rectum and ε is the eccentricity of the ellipse.

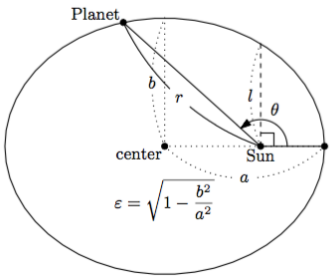


Figure 1: Elliptical orbit of the planet.

2. A line segment joining a planet and the Sun sweeps out equal areas during equal intervals of time. Because the planetary area velocity $\frac{dS}{dt}$ is constant, we obtain the following formula.

$$\frac{dS}{dt} = \frac{1}{2}r^2\frac{d\theta}{dt} = \kappa \ \ (\text{Kepler}'\text{s constant}) \tag{2}$$

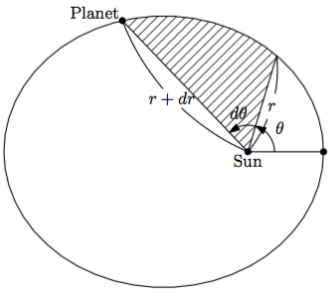


Figure 2: Planetary swept area.

3. The square of the orbital period of a planet is proportional to the cube of the semi-major axis of its orbit. Letting T be the orbital period and letting a the elliptical semi-major axis, then T and a satisfy the following condition.

$$\frac{T^2}{a^3} = C \ \ (\text{constant}) \tag{3}$$

In 1687, I. Newton derived Kepler's laws from the law of universal gravitation in his book "The Principia"[2].

Using KeTCindy, the authors calculate the planetary swept area as

$$2\kappa t = \int_0^t r^2 \frac{d\theta}{dt}\, dt = \int_0^t \frac{l^2}{(1+\varepsilon\, \cos\theta)^2}\, d\theta \tag{4}$$

and the planetary velocity vector

$$\frac{dx}{dt} = 2\kappa \left(\frac{\varepsilon \sin\theta \cos\theta}{l} - \frac{\sin\theta}{r} \right), \frac{dy}{dt} = 2\kappa \left(\frac{\varepsilon \sin^2\theta}{l} + \frac{\cos\theta}{r} \right) \tag{5}$$

and planetary acceleration vector, respectively, from Kepler's first law (1). Subsequently, they exhibit the calculated planetary motion so that the planetary area velocity is constant.

Keywords: Orbits of planets, Cinderella, Maxima, TeX, KeTCindy

References

[1] S. YAMASHITA; S. KOBAYASHI; H. MAKISHITA; S. TAKATO, PDF Slide Teaching Materials Created Using KeTCindy. In *Computer Science and Its Applications – ICCSA2017*, O. Gervasi et al. (eds.), pp.285–300, Springer, Italy, 2017.

[2] I. BERNARD; A. WHITMAN, *Isaac Newton, The Principia – Mathematical Principles of Natural Philosophy*. University of California Press, London, 1999.

[1]Department of Natural Science,
National Institute of Technology, Kisarazu College
2-11-1, Kiyomidai-Higashi, Kisarazu, 292-0041, Japan
yamasita@kisarazu.ac.jp

[2]Division of Liberal Arts
Kogakuin University
2665-1 Nakano, Hachioji, Tokyo 192-0015, Japan
kitahara@cc.kogakuin.ac.jp

[3]Department of Informatics, Faculty of Informatics,
Tokyo University of Information Sciences
4-1, Onari-dai, Wakaba-ku, Chiba, 265-8501, Japan
miyake.shuhei@gmail.com

[4]Department of Science,
Toho University
2-2-1, Miyama, Funabashi, 274-8510, Japan
takato@phar.toho-u.ac.jp

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Fluid/Particles Flow Simulation by Finite Volume Method -Hybrid Approach-

Salah ZOUAOUI[1], **Hassane DJEBOURI**[1], **Ali BILEK**[1] and **Kamal MOHAMMEDI**[2]

We present here a numerical method to compute the motion of rigid particles in fluid flow with a non-elastic impact law. Many methods have been proposed recently and different strategies have been used to compute such flows [1]. Our motivation is the handling of the non-overlapping constraint in fluid-particle direct simulations [2, 3]. Each particle is treated individually and the Navier-Stokes equations are solved for the moving fluid by Fluent code which is based on the Finite volume method. The contact-handling algorithm is based on the projection of the velocity field of the rigid particles over the velocity field of the fluid flow. The method consists of imposing a constraint on the velocity field of the particles, as a guarantee that at each time step the calculated particle velocity field belongs to an eligible velocity field of the fluid. In this case study, an Uzawa algorithm has been applied [4].

Keywords: Simulation, Flow, Particles, Contact, Uzawa, Fluent

Contact Handling Procedure

Let us detail the method in the case of spherical particles: we denote by $\mathbf{X}^n := (\mathrm{x}_\mathrm{i}^\mathrm{n})_{i=1,.....,N}$ the position of N particles (more precisely, the position of their gravity centre) at time t_n, by $\hat{\mathbf{V}}^n = (\hat{\mathrm{v}}_i)_{i=1,.....,N}$ the a priori translational velocity, by $\hat{\Omega}^n = (\hat{\omega}_i)_{i=1,.....,N}$ the a priori rotational velocity. As stated before, the a priori updated position of the particles, defined as:

$$\mathbf{X}^{n+1} = \mathbf{X}^n + \Delta t \hat{\mathbf{V}}^n + \frac{1}{2}\gamma^n \triangle t^2 \tag{1}$$

where γ the acceleration, calculated from the Newton's second law. Equation 1 may lead to non-admissible configuration, in the sense that the particles overlap. To avoid this, we project the velocities onto the following set:

$$K(X^n) = \{\mathrm{V} \in \mathbb{R}^{2N}, D_{ij}(\mathrm{X}^n) + \Delta t \mathrm{G}_{ij}(\mathrm{X}^n).\mathrm{V} + \frac{1}{2}\gamma^n \triangle t^2 \geqslant 0, \forall i < j\} \tag{2}$$

where D_{ij} is the distance between every two particles given as:

$$D_{ij}(\mathrm{X}^n) = \|\mathrm{x}_i^n - \mathrm{x}_j^n\| - (R_i - R_j) \tag{3}$$

At each time step, $\mathrm{V} \in \mathbb{R}^{2N}$ is an admissible vector if the particles with velocity $\{\mathrm{V}$ do not overlap at the next time step:

$$E(X^n) = \{\mathrm{V} \in \mathbb{R}^{2N}, D_{ij}(\mathrm{X}^n + \Delta t \mathrm{V}^n + \frac{1}{2}\gamma^n \triangle t^2) \geqslant 0, \forall i < j\} \tag{4}$$

We not that equation 2 is the linearized form of equation 4 and, furthermore, it can be shown that $K(X^n) \subset E(X^n)$. It means in particular that particles with admissible velocities at time t_n do not overlap at time t_{n+1}.
The constrained problem is formulated as a saddle-point problem, by using the introduction of Lagrange multipliers:

$$\begin{cases} Find(\mathrm{V}^n, \Lambda^n) \in \mathbb{R}^{2N} \times \mathbb{R}_+^{N(N-1)/2} \quad suchthat \\ \mathcal{J}(\mathrm{V}^n, \lambda) \leqslant \mathcal{J}(\mathrm{V}^n, \Lambda^n) \leqslant \mathcal{J}(\mathrm{V}, \Lambda^n), \quad \forall (\mathrm{V}^n, \lambda) \in \mathbb{R}^{2N} \times \mathbb{R}_+^{N(N-1)/2} \end{cases} \tag{5}$$

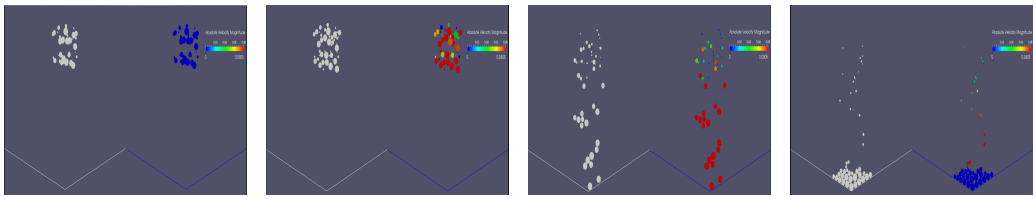
with the following functional:

$$\mathcal{J}(\mathrm{V}, \lambda) = \frac{1}{2} \mid \mathrm{V} - \hat{\mathbf{V}}^n \mid^2 - \sum_{1 \leqslant i \leqslant j \leqslant N} \lambda_{ij}(D_{ij}(\mathrm{X}^n) + \Delta t \mathrm{G}_{ij}(\mathrm{X}^n).\mathrm{V}) + \frac{1}{2}\gamma^n \triangle t^2 \tag{6}$$

Where $\mathrm{G}_{ij}(\mathrm{X}^n) \in \mathbb{R}^{2N}$ is the gradient of distance D_{ij}. The number of Lagrange multipliers (λ_{ij}) corresponds to the number of possible contacts. This problem is solved by an Uzawa algorithm.

Falling of 50 particles of different sizes on a plane

The computer implementation of the contact Handling algorithm allows us to simulate the falling of 50 particles of different sizes on a plane (figure1). This allows us to highlight the particle/particle and particle/wall contact.



$t = 0.0s$ $t = 0.10s$ $t = 0.20s$ $t = 0.80s$

Figure 1: Fall down of 50 particles of different sizes on a plane

Simulation of the water flow inside a pipe with obstacles

The incompressible Navier-Stokes equations are written in the following form.

$$\begin{cases} \rho_f \dfrac{Du}{Dt} - \mu \Delta u + \nabla p = f_{\ \Omega \backslash \overline{B}} & \text{dans } \Omega \\ \nabla . u = 0 & \text{dans } \Omega \\ u = 0 & \text{sur } \partial\Omega \end{cases} \tag{7}$$

where ρ_{f} denotes the density of the fluid, $\mathrm{u}(u_1, u_2)$ the velocity of fluid, σ the stress tensor and $\mathbf{f}_{\mathrm{f}} = \rho_{\mathrm{f}}\, g e_y$ is the external force exerted on the fluid (gravity forces). We used a Fluent commercial code to solve equation 7.

Fluid-Particles Simulation

In this test case, we simulated the transport of solid particles in a pipe with obstacles (figure 2). To take into account the solid particles we integrated, in the code of contact management, the equations of the solid dynamics by considering all the forces acting on a particle in a fluid flow. On the other hand, for the numerical resolution of the Navier-Stokes equations, we resorted to the use of a Fluent commercial code which is based on the finite volume method.

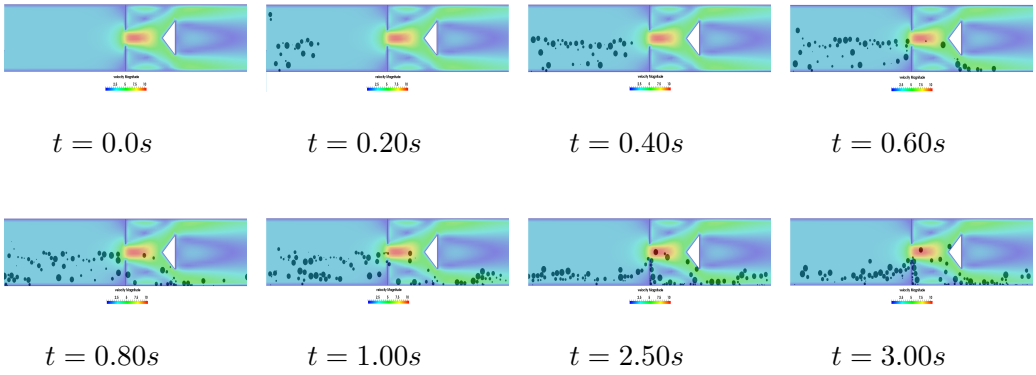


Figure 2: Injection of solid particles: Configuration at different time steps

References

[1] ZOUAOUI, S., DJEBOURI, H., BILEK, A. ET AL., Modelling and Simulation of Solid Particle Sedimentation in an Incompressible Newtonian Fluid. *Math.Comput.Sci.* **11**(3-4), 527–539 (2017).

[2] MAURY, B., A time-stepping scheme for inelastic collisions. *Numerische Mathematik* **102**(4), 649—679 (2006).

[3] ALINE LEFEBVRE., Fluid-particle simulations with freefem++. *InESAIM: Proceedings* **18**(4), 120—132 (2007).

[4] BANK, R.,WELFERT, B., AND YSERENTANT, H.,A class of iterative methods for solving saddle point problems. *Numerische Mathematik* **56**(7), 645–666. (1989).

[1]LMSE Laboratory
Mechanical Engineering Department
Mouloud Mammeri University of Tizi-Ouzou
P.O. Box17 RP, 15000 Tizi Ouzou, Algeria
zouaoui_salah2003@yahoo.fr; zouaouisalah@ummto.dz

[2]Unité de Recherche Matériaux, Procédés et Environnement (URMPE)
MESOnexusteam
Université M'hamed Bougara Boumerdès
Algérie 35000
mohammedik@yahoo.com

S3
Computer Algebra in Education

Education has become one of the fastest growing application areas for computers in general and computer algebra in particular. Computer Algebra Systems (CAS) make for powerful teaching and learning tools within mathematics, physics, chemistry, biology, economics, etc. Among them are:

- the commercial "heavy weights" such as Casio ClassPad 330, Derive, Magma, Maple, Mathematica, MuPAD, TI NSpire CAS, and
- the free software/open source systems such as Axiom, Euler, Fermat, wxMaxima, Reduce, and the rising stars such as GeoGebra, Sage, SymPy and Xcas (the swiss knife for mathematics).

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

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

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

New rules for improving CAS capabilities when computing improper integrals. Applications in Math Education

José Luis Galán-García[1], **Gabriel Aguilera-Venegas**[1], **Pedro Rodríguez-Cielos**[1], **Yolanda Padilla-Domínguez**[1], **María Ángeles Galán-García**[1]

In many Engineering applications the computation of improper integrals is a need. In [1] we pointed out the lack of some CAS when computing some types of improper integrals. Even more, the work developed showed that some improper integrals can not be computed with CAS using their build-in procedures.

In this talk we will develop new rules to improve CAS capabilities in order to compute improper integrals such as:

1. $\displaystyle\int_0^\infty f(x)\,g(x)\mathrm{d}x$; $\displaystyle\int_{-\infty}^0 f(x)\,g(x)\mathrm{d}x$ and $\displaystyle\int_{-\infty}^\infty f(x)\,g(x)\mathrm{d}x$

   where $g(x)=1$ or $g(x)=\sin(ax)$ or $g(x)=\cos(ax)$ and $f(x)=\dfrac{p(x)}{q(x)}$ with degree of $p(x)$ smaller than degree of $q(x)$ and $q(x)$ with no real roots of order greater than 1.

2. $\displaystyle\int_0^\infty x^\alpha\,f(x)\,\mathrm{d}x$ where $\alpha\in\mathbb{R}\setminus\mathbb{Z}$ or $-1<\alpha<0$

We will show examples of improper integrals that CAS as MATHEMATICA, MAPLE, DERIVE or MAXIMA cannot compute. Using advance techniques as Laplace and Fourier transforms or Residue Theorem in Complex Analysis, we can develop new rules schemes for these improper integrals. We will also describe the conclusions obtained after using these new rules with our Engineering students when teaching Advanced Calculus.

Keywords: Improper Integrals, Rules Development, CAS, Engineering

References

[1] José L.Galán-García, Gabriel Aguilera-Venegas, María Á. Galán-García, Pedro Rodríguez-Cielos, Iván Atencia-Mc.Killop. Improving CAS capabilities: New rules for computing improper integrals. Applied Mathematics and Computation. Volume 316, 1 January 2018, Pages 525-540.

[1]Departamento de Matemática Aplicada. University of Málaga.
jlgalan@uma.es

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Teaching Partial Differential Equations with CAS

José Luis Galán-García[1], **Pedro Rodríguez-Cielos**[1], **Yolanda Padilla-Domínguez**[1], **María Ángeles Galán-García**[1], **Gabriel Aguilera-Venegas**[1], **Ricardo Rodríguez-Cielos**[2]

Partial Differential Equations (PDE) are one of the topics where Engineering students find more difficulties when facing Math subjects.

A basic course in Partial Differential Equations (PDE) in Engineering, usually deals at least, with the following PDE problems:

1. **Pfaff Differential Equations**, which consists on finding the general solution for:
$$P(x,y,z)\,\mathrm{d}x + Q(x,y,z)\,\mathrm{d}y + R(x,y,z)\,\mathrm{d}z = 0$$

2. **Quasi-linear Partial Differential Equations**, which consists on finding the general solution for: $P(x,y,x)\,p + Q(x,y,z)\,q = R(x,y,z)$ where $p = \dfrac{\partial\, z}{\partial\, x}$ and $q = \dfrac{\partial\, z}{\partial\, y}$.

3. Using **Lagrange-Charpit Method** for finding a *complete integral* for a given general first order partial differential equation: $F(x,y,z,p,q) = 0$.

4. **Heat equation** which consists on solving the second order PDE:
$$\begin{cases} k\dfrac{\partial^2 u}{\partial x^2} = \dfrac{\partial u}{\partial t}, \quad k>0 & 0<x<L & t>0 \\ u(0,t) = 0 & u(L,t) = 0 & t>0 \\ u(x,0) = f(x) & 0<x<L & \end{cases}$$

5. **Wave equation** which consists on solving the second order PDE:
$$\begin{cases} a^2\,\dfrac{\partial^2 u}{\partial x^2} = \dfrac{\partial^2 u}{\partial t^2} & 0<x<L & t>0 \\ u(0,t) = 0 & u(L,t) = 0 & t\geq 0 \\ u(x,0) = f(x) & \left.\dfrac{\partial u}{\partial t}\right|_{t=0} = g(x) & 0<x<L \end{cases}$$

6. **Laplace's equation** which consists on solving the second order PDE:

$$\begin{cases} \dfrac{\partial^2 u}{\partial x^2} + \dfrac{\partial^2 u}{\partial y^2} = 0 & 0 < x < a & 0 < y < b \\ \left.\dfrac{\partial u}{\partial x}\right|_{x=0} = 0 & \left.\dfrac{\partial u}{\partial x}\right|_{x=a} = 0 & 0 < y < b \\ u(x,0) = 0 & u(x,b) = f(x) & 0 < x < a \end{cases}$$

In this talk we will describe how we introduce CAS in the teaching of PDE.

The tasks developed combine the power of a CAS with the flexibility of programming with it. Specifically, we use the CAS DERIVE. The use of programming allows us to use DERIVE as a Pedagogical CAS (PECAS) in the sense that we do not only provide the final result of an exercise but also display all the intermediate steps which lead to find the solution of a problem. This way, the library developed in DERIVE serves as a tutorial showing, step by step, the way to face PDE exercises.

In the process of solving PDE exercises, first-order Ordinary Differential Equations (ODE) are needed. The programs developed can be grouped within the following blocks:

- **First-order ODE**: separable equations and equations reducible to them, homogeneous equations and equations reducible to them, exact differential equations and equations reducible to them (integrating factor technique), linear equations, the Bernoulli equation, the Riccati equation, First-order differential equations and nth degree in y', Generic programs to solve first order differential equations.
- **First-order PDE**: Pfaff Differential Equations, Quasi-linear PDE, Lagrange-Charpit Method for First-order PDE.
- **Second-order PDE**: Heat Equation, Wave Equation, Laplace's Equation.

In this talk we will introduce some improvements (redefinition of programs and more types of ODE and PDE) with respect to the talks given in previous ACA [1, 2] related with these topics. We will also remark the conclusions obtained after using these techniques with our Engineering students.

Keywords: ODE, PDE, DERIVE, CAS, PECAS, Engineering

References

[1] Gabriel Aguilera, José Luis Galán, M. Ángeles Galán, Antonio Gálvez, Antonio J. Jiménez, Yolanda Padilla, Pedro Rodríguez. DIFFERENTIAL EQUATIONS WITH DERIVE 6. Applications of Computer Algebra Conference, ACA 2008 (Computer Algebra in Education Session), http://math.unm.edu/∼aca/ACA/2008/Proceedings/Education/Galan_abstract.pdf.

[2] G. Aguilera, J.L. Galán, M.A. Galán, Y. Padilla, P. Rodríguez, R. Rodríguez. FOPDE.mth: Solving First-Order Partial Differential Equations with DERIVE 6 step by step. Proceedings of the International Conference on Applications of Computer Algebra (ACA 2013). 2013. I.S.B.N. 978–84–616–4565–7.

[1]Departamento de Matemática Aplicada. University of Málaga.
jlgalan@uma.es

[2]Departamento de Señales, Sistemas y Radicomunicaciones. Technical University of Madrid.

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

About the Bulgarian experience in organizing National Student Olympiad in Computer Mathematics

Penka Georgieva[1]

In this paper the experience in organizing, conducting and participating in the National Student Olympiad in Computer Mathematics "Acad. Stefan Dodunekov" (CompMath) in Bulgaria is presented.

CompMath has been running since 2009. The first two olympiads were experimental. Since 2011 it is in the competitions calendar of Bulgarian universities. The idea is to promote the tools of computer algebra software and inspire the academic community to be part of this Olympiad [1].

CompMath is organized annually, it is held by a National Committee (NC) and hosted by a different university every year. A General Assembly of CompMath consists of the team leaders from the participating universities and meets at least once a year. Every university student enrolled in a bachelor or master degree programme at a Bulgarian or foreign university can participate individually. The participants are divided into groups: Group A - Mathematics, Informatics and Computer Science, Group B - Engineering and Natural Science. Those in group B are allowed to compete in Group A. In the last year there was one more group for school mathematics, again experimentally. Ranking is done within each Group. Up to 50 percents of the participants are awarded golden, silver or bronze medals by the NC in an approximate ratio of $1 : 2 : 3$. The Organizing Committee issues certificates for the participants and team leaders [2].

Thirty problems from different areas of mathematics (Algebra, Analytic Geometry, Calculus, Differential Equations, Probability theory, etc.) have to be solved within 4 hours. Twenty of the problems can be solved using basic CAS functions, the remaining ten require advanced knowledge and skills.

The participants are free to choose the technology they prefer. They are allowed to use only one CAS, Matlab and also to combine two or more CAS, CAS and Matlab. Some students use only Mathematica, other - MatLab and MuPad, engineering students prefer Maple, Matlab and MuPaD.

Rapid changes in computer and information technology and the large number of mathematical software are prerequisites for gradual changes in the teaching and learning of university mathematics. The CompMath is a step towards these changes at Bulgarian universities.

Keywords: Computer mathematics, Olympiad, Bulgarian experience

This paper is partially supported by the project $D14-2305$ "Modern software engineering products for scientific research - training for lecturers and students in Faculty of Computer Science and Engineering and Faculty of Business Studies, Burgas Free University", "University Research Fund", BFU $2017/2018$.

References

[1] www.compmath.eu/2017/

[2] www.compmath.eu/2017/docs/regulations_en.pdf

[1]Burgas Free University
San Stefano Str. 62, Burgas 8001, Bulgaria
penka.georgieva@bfu.bg

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Do we take advantage of ICT when teaching maths at primary and secondary education levels? Do we teach maths as we should?

Eugenio Roanes-Lozano[1]

My son is finishing primary education and I consider many of the school activities he has undertaken a waste of time. For example, does it make sense to divide by hand a twelve-digit number by a seven-digit number, or to factorize by hand an integer, two of whose factors are 71 and 107?

Although these are very specific cases, the exercises proposed in math classes at the primary and secondary education levels are not usually interesting, are sometimes even tedious and do not make the student love but hate maths. For example, in the case of factoring a number, the key is to understand what is being done and to know how to do it (algorithm), but it makes no sense to resolve uncomfortable cases when powerful computer algebra systems (CAS) are available in computers, calculators and even smartphones. In addition, the exercises proposed are many times disconnected from the real world (unlike many of those proposed in tests such as Pisa).

The use of ICT (at least in Spain) is many times restricted to "doing some research" on certain specific topics, but this is often a euphemism, since what the student many times does is just a "Google search".

Almost twenty years ago a secondary schoolmate asked me which software to use, since the computers of his school had only the operating system and an office package and there were no funds for software. My answer was taxative: the CAS Maxima and the (then new) dynamic geometry system (DGS) GeoGebra. GeoGebra has spread considerably at secondary education level (overshadowing the pioneers Cabri Géomètre and The Geometer's Sketchpad and the other DGS), but no CAS has clearly spread at this level. Possibly, the use of the latter has even decreased at this level for two reasons:

- Derive being discontinued
- the incorporation of algebraic capabilities by GeoGebra.

Despite the fact that since the 90s different theories have been developed about the use of mathematical software in education, such as the "Black Box / Whyte Box Principle" [1,2] and the "Mathematical Creativity Spiral" [3] (Buchberger), the "Scaffolding Principle" [4] (Kutzler) or the "Elevator Principle" [5] (Cabezas and Roanes), the teaching of primary and secondary education level mathematics continues to have a very low level of experimentality and the intensive use of mathematical software in the classes is exceptional.

Which can be the reasons for the limited use of ICT in the math classes and the persistence of tedious activities?

Keywords: Computational mathematics, Mathematical education

References

[1] B. BUCHBERGER, Should students learn integration rules? *SIGSAM Bulletin* **24**(1), 10–17 (1990). DOI 10.1145/382276.1095228.

[2] P. DRIJVERS, White-box/black-box revisited. *The International DERIVE Journal* **2**(1), 3–14 (1995).

[3] B. BUCHBERGER, The Creativity Spiral in Mathematics. *RISC Linz Technical Report No. 92, University of Linz* (1992).

[4] B. KUTZLER, *Improving Mathematics Teaching with DERIVE*. Chartwell-Bratt, Bromley, Kent, UK, 1996.

[5] JUSTO CABEZAS-CORCHERO; EUGENIO ROANES-LOZANO, Four Experiences and Some Reflections about the Influence of Mathematical Software on the Mathematics Curriculum. *Journal of Scientific Research and Reports* **7**(2), 154–164 (2015). DOI 10.9734/JSRR/2015/17798.

[1]Instituto de Matemática Interdisciplinar &
Depto. de Álgebra, Geometría y Topología
Facultad de Educación, Universidad Complutense de Madrid
c/ Rector Royo Villanova s/n, 28040-Madrid, Spain
eroanes@mat.ucm.es

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Technology enhanced e-assessments in Calculus courses with application of CAS

Elena Varbanova[1]

1. About the changing face of engineering education

As long as education can change, the world can change.

The technological development in the twenty-first century naturally and inevitably leads to the introduction of new tools into the university education. The experience in e-learning at the Technical University of Sofia (TUS) can be traced back to 1998. Numerous technology enhanced lectures, tutorials, laboratory classes and related textbooks have been created by lecturers in engineering, informatics and mathematics courses. Students and PhD students have been also involved through the development of theses on applications of Virtual Learning Environments (VLE) such as Moodle and ILIAS for design and implementation of effective didactic models. The outcomes of their research contribute to the changing face of engineering education.

Mathematics education has undergone a transformation based on applications of Computer Algebra Systems (CAS) [2], [3] and VLE. Though their simultaneous application is a challenge, it is a good opportunity for digitalizing mathematics education. Actually, there is "no way back", i.e. no education, progress and development without technology. Digital mathematics exists and digital resistance is not appropriate.

The focus of a dynamic unity of VLE and CAS in mathematics courses at TUS was on students' motivated, active, conscious and emotional participation in the teaching-learning-assessment (TLA) process. Assessment was an integral part of the TLA process and the three components were equally considered and mutually interrelated. But something was missing in the digital environment . . . It was e-assessments (diagnostic, continuous, formative, summative) provided with tools for authentication & authorship analysis in online and blended environments assuming the student would take the assessment at a distance. And, finally, a brave but necessary project TeSLA has arrived [5].

2. Re-design of Calculus courses within the framework of TeSLA project

Ne varietatem timeamus. /Do not be afraid of diversity./

Since January 2016 TUS is a partner university in the TeSLA project which conception /philosophy/ is built on a "general trust" that knows no time limits or national

boundaries and could fit to any system of higher education. The project aims to support and assure e-assessment processes in order to improve the trust level across students, teachers and institutions. According to TeSLA LOGO this system provides continuous and modular trust-based authentication & authorship analysis for e-assessments.

Concerning the educational aspects of TeSLA system it has to be mentioned that its implementation could give a significant added value as well: highly qualified and experienced teachers can design and develop a great diversity of e-assessment activities with purposeful and balanced application of the potential of the VLE and course related software [1], [4]. And these cannot be achieved in a face-to-face educational mode. Of course, teachers have to be aware of possible abuse of technology: they have to make what is important technology supported, rather than what is technology-supported important.

The undergraduate course Calculus 1 (Calculus of One Variable) was one of the piloted courses in TeSLA project. It is taught to students first year of study. The latter could be a reason they to prefer performing the activities in university computer labs, not at home, i.e. not at a distance. Within the framework of TeSLA project six tools for authentication & authorship analysis have been developed and tested in seven partner universities. Understandably, *Face Recognition* (*FR*) and *Keystroke Dynamics* (*KD*) were recommended to be tested as suitable for mathematics courses. Another two named *Voice Recognition* and *Plagiarism* are also useful for assessing students' capability to defense their individual and collaborative courseworks or to explain multi-step solutions. In the presentation a real (follow up) assessment activity monitored by TeSLa system will be demonstrated.

The students performed three activities: enrolment and two follow-up assessment activities. It was both challenging and exciting to re-design the TLA process, modify existing in-class tests and re-formulate questions. On one hand, in order to enhance the quality of assessment activities, we took advantage of the wide range of types of questions available in VLE Moodle and used the potential of a CAS-environment to create questions as well as to facilitate students in selection of approaches to find, interpret and check up answers/solutions. On the other hand, appropriate support materials were provided online and students could use also external resources.

Almost all the types of questions available in VLE Moodle were included in the assessment activities: True/False, Numerical, Multiple choice, Matching, Drag and drop into text, Drag and drop onto image, Select missing words, Essay /open answer questions/. A didactic system of questions/problems has been created. This diversity of questions and flexibility in answering them considerably contributed to enrichment and enhancement of assessment activities. They could serve as innovative assessment practices in mathematics education. During the assessment process students are allowed/required to use CAS and submit the produced CAS-protocol with solutions, explanations, interpretations and reflection on the results. In the presentation illustrative examples will be shown.

3. The synergies between VLE, CAS and TeSLA tools for enhancing university mathematics

Some things can't be explained, only experienced.

All the three components of the triad teaching-learning-assessment are to be considered in tandem and not focus on any one of them. Through a balanced integration of VLE and CAS in the design and development of assessment activities and related learning and support materials we aimed at helping students built up habits for Lower Order Learning and Higher Order Learning in accordance with the improved Bloom's taxonomy.

The follow up activities were performed by students for the purpose of formative e-assessment. They were used for both summative purposes in that 20% of the overall mark was allocated to these activities and formatively in that detailed feedback was provided. The latter appeared to be a motivation for students to better prepare themselves and avoid attempts for "helping" classmates or using illegal ways far achieving higher results. Universities have a mission to create a good sense of fairness and honesty for students as an important element of culture and to ensure action. And here TeSLA tools come to the rescue.

An e-assessment tool provides data to teachers about students. Having information per student, and also per "classroom", teachers could propose changes in courses and curriculum in order to help students acquire sustainable knowledge and develop required competencies. Independent individual/collaborative learning with self-assessment can also be monitored by TeSLA tools. On time provided feedback both online and offline, based on the individual learning trajectory, allows students make a desired progress in their own pace anytime and anywhere.

4. Conclusion

Challenge is energy of life.

Technology can "replace" hundreds of teachers but a powerful methodology and highly qualified teachers can give thousands of technologies vitality. Training of teachers should be the key concern of universities: in creation of e-assessment activities interrelated with the teaching and learning activities and according to the principle "What gets assessed is what gets taught". Like any other technological tool TeSLA system need a professional attitude to be taken to. Converting tools into effectively integrable instruments is a real question in education. In this sense there is still much to be done in order to assure trust-based e-assessments.

Educational technology (ET) is to be considered as

ET=Technology OF Education+Technology IN Education.

A proper utilization of technology in education requires a policy of support for research in the field of educational science, high quality software and teacher training. Together we need to go further to 4C = Challenging Changes in Curricula and Courses.

Keywords: mathematics education, e-assessment, CAS, VLE, TeSLA system

References

[1] E. A. VARBANOVA, CAS supported environment for learning and teaching calculus. *CBMS Issues in Mathematics Education: Enhancing University Mathematics*, **14**, AMS&MAA, (2007).

[2] E. VARBANOVA, *Calculus 1. Lecture Notes*. TU-Sofia, Sofia, 2009 (in Bulgarian).

[3] E. VARBANOVA, *Calculus 1. Exercises*. TU-Sofia, Sofia, 2011 (in Bulgarian).

[4] E. VARBANOVA, About Balanced Application of CAS in Undergraduate Mathematics. *Applications of Computer Algebra, Springer Proceedings in Mathematics & Statistics 198*. Springer International Publishing AG, 2017.

[5] http://www.tesla-project.eu

[1]Faculty of applied mathematics and informatics
Technical University of Sofia
Kliment Ohridski Blvd. 8, Sofia 1000, Bulgaria
elvar@tu-sofia.bg

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Analyzing the "Calculator Effect" of Different Kinds of Software for School Arithmetics and Algebra

Rein Prank[1]

The author of this paper realised the need to think about misuse effects when participating in two activities connecting Mathematics teaching and computers: addition of school-style step by step solutions to the output of CAS, and compiling a workbook that contains programming tasks extracted from School Mathematics.

The possibility of getting the answer and solution of arithmetic and algebra tasks from external sources is currently provided by four kinds of software:

1. **Spreadsheets.** We usually think that spreadsheets do decimal calculations. Solving examples from School Mathematics demonstrates an unexpected and undocumented mixture of decimal and algebraic calculations.

2. **Lightweight drill environments** for arithmetic and algebra. They have quite small calculator effect because usually they do not enable entering user-provided exercises.

3. **Step by step solution environments** (MathXpert, Aplusix, T-algebra). The key question is again whether the student gets right to enter initial expressions of the tasks.

4. **"Algebra calculators".** There are a few dozen programs designed specifically for doing students' homework (producing solutions with necessary explanations) for almost all technical exercises of School Algebra. But very often the calculators implement textbook algorithms without any intelligence.

Item 4 means that availability of solutions in educational CAS (for example, in Geogebra) will not change the situation very much. In the first years, the CAS solutions will most likely have the same imperfections as the current algebra calculators.

Many school arithmetic and algebra tasks can be converted to programming tasks: long multiplication or division, reducing fractions, multiplication of polynomials. For routine tasks, programming does not replace exercising with something easier. The situation can be different when we come to the more original tasks in textbooks. A task of replacing stars with given numbers can lead to an interesting logical journey. However, stronger students in middle grades are perfectly capable of programming a brute-force solution search. It is important to think about ways of protecting the more interesting tasks in textbooks from such shortcuts.

Keywords: Calculator effect, Computer algebra, School Mathematics

[1]Institute of Computer Science
University of Tartu
Liivi Str 2, Tartu, Estonia
rein.prank@ut.ee

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Student Attitudes toward Technology Use in Math Education

Karsten Schmidt[1]

In the Faculty of Business and Economics at Schmalkalden University, the matrix algebra course of the bachelor program has been taught in the PC lab for many years (one or two students in front of a PC, instructor's PC connected to a projector). A Computer Algebra System (CAS) is used throughout the course. Students can install the CAS on their private PCs, and have access to it during the final exam in the PC lab (then, naturally, only one student per PC). Other courses, like Introduction to Mathematics, and Introduction to Statistics, are still taught in a traditional classroom setting (blackboard, overhead projector, and pocket calculators). At the beginning of the 2010/11 winter semester, a survey was carried out to investigate whether the students preferred traditional or technology-based courses in mathematics, and how well they coped with the technology. During the 2015/16 winter semester, a similar survey was carried out to check whether students' attitudes toward the use of technology in the teaching of mathematics have changed over time. In this presentation we will look at the key questions of the questionnaire, display descriptive statistics as well as charts of the variables generated from the gathered data, and analyze the effect that certain characteristics of the students (e.g. male vs. female, or students who like math vs. those who do not) have on their answers. The new results will be also compared to those found five years ago.

Keywords: Student attitude toward CAS, Survey of students, Changes over time

References

[1] K. SCHMIDT; A. KÖHLER, *Teaching mathematics in the PC lab – the students'viewpoints*, International Journal of Mathematical Education in Science and Technology, **44**(3), 317–331 (2013).

[1]Faculty of Business and Economics
Schmalkalden University of Applied Sciences
Blechhammer, 98574 Schmalkalden, Germany
kschmidt@hs-sm.de

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Dynamic visualizations for network flow optimizations problems with Mathematica

Włodzimierz Wojas[1], **Jan Krupa**[1]

Network flows as a problem domain is considered as a part of such mathematical disciplines as: graph theory, combinatorial optimization, mathematical programming or operation research. It is taught at universities in framework of different academic courses, for example: Graphs and networks, Optimization methods, Linear programming, Mathematical programming or Operation research. In the framework of network flows a number of optimizations problems are considered, such as: shortest path problem, maximum flow problem or minimum cost flow problem. Newer versions of Mathematica contain some functions dedicate to solve some network flows optimizations problems. In this talk, first we would like to present a few dynamic visualizations of network flows in pure, generalized and dynamic networks using Mathematica. Next, we will present visualizations for maximum flow problem and minimum cost flow problem

Keywords: network flows, network optimization, didactics of mathematics, mathematics education, CAS, Mathematica

References

[1] R. K. Ahuja, T. L. Magnanti, and J. B. Orlin, *Network Flows: theory, algorithms, and applications*, Prentice Hall, (1993)

[2] L.R. Ford, D.R. Fulkerson, *Network Flows* Princeton University Press, (1962)

[3] http://reference.wolfram.com/language/ref/FindMaximumFlow.html

[4] http://reference.wolfram.com/language/ref/FindMinimumCostFlow.html

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

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

[1]Department of Applied Mathematics
Warsaw University of Life Sciences (SGGW)
Warsaw Poland
wlodzimierz_wojas@sggw.pl
jan_krupa@sggw.pl

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Using TI-Nspire for the financial education of future engineers

Hanan Smidi[1]

For several years, and more precisely since September 2011, "L'École de technologie supérieure" (ÉTS) has chosen the TI-Nspire as the mandatory calculator for most, if not, all courses leading to an engineering degree.

One compulsory course in particular requires students to learn about the financial profitability of a project. The TI-Nspire offers all the basic financial functions from calculating the time value of money, depreciation of a loan, solving complex equations, graphic representations as well as programming functions for a quicker and easier access.

With its software, the lecturer can easily show examples while students can follow and do the problems directly on their handheld devices in the classroom.

There are many financial calculators available and mostly, Excel is widely used to present financial models. The TI-Nspire allows the user to solve most financial math situations on one device and hence become an unavoidable and powerful tool for the student.

This short presentation is an overview of the TI-Nspire's powerful use of financial math in the classroom.

[1]Senior lecturer, Service des enseignements généraux
École de technologie supérieure, Université du Québec
1100 Notre-Dame street West, Montréal, Québec, Canada, H3C 1K3
hanan.smidi@etsmtl.ca

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Accurate plotting in 3D: how to choose the mesh

David G. Zeitoun[1], **Thierry N. Dana-Picard**[2]

When studying continuity of 1-variable functions, a classical example is given by the function f such that $f(x) = \sin \frac{1}{x}$. this is an opportunity to show an example of Heine's Theorem:

Theorem: *Let f be a function defined on a punctured neighborhood of the real number a. The two following properties are equivalent:*

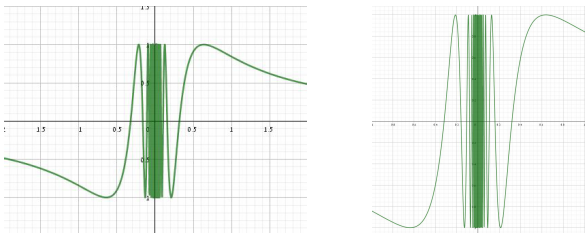
1. *The function f has a limit l at a (maybe infinite).*
2. *For every convergent sequence (x_n) of real numbers whose limit is a, the sequence $(f(x_n))$ has limit l.*

Take the sequences given by

$$x_n = \frac{1}{2n\pi} \text{ and } y_n = \frac{1}{2n\pi + \frac{\pi}{2}}$$

Both sequences converge and have a limit equal to 0, but $f(x_n)$ and $f(y_n)$ have different limits, showing that f has a discontinuity at 0.

This situation cannot be illustrated using a plot. Figure 1 shows the strange plot obtained using a standard command*. Zooming does not improve the visualization, as the function has an infinite number of oscillations within a compact interval around 0. Students have difficulties both with the visualization and with "for every sequence". The teacher has to insist on the fact that this theorem is mostly used to disprove continuity/existence of a limit.



(a) First plot (b) After zooming

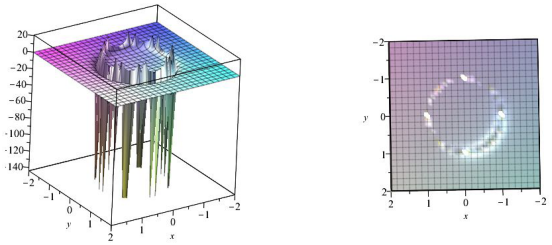
Figure 1: Strange plots for a one-variable function

*We used GeoGebra, but the same phenomenon appears with any other package.

Transition towards Calculus II, with functions of 2 real variables (or more than two) leads to problems, either different or more of the same. Sometimes, the visualization becomes harder to understand. For example, consider the function given by

$$f(x,y) = \frac{1}{1-(x^2+y^2)}. \tag{1}$$

Using standard commands for plotting graphs of 2-variable functions may provide a non accurate result (see Figure 2).



(a) (b)

Figure 2: Strange plots for a two-variable function

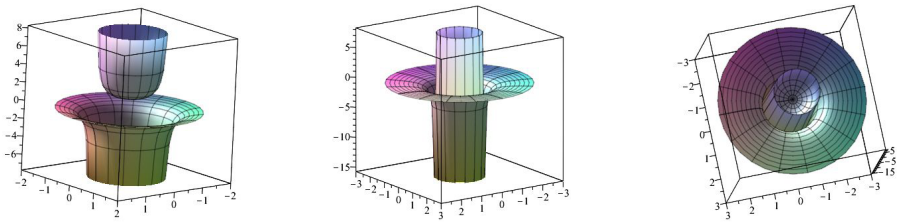
The function has non-isolated singularities, but the plot in cartesian coordinates does not show them. Moreover the plot shows a lot of needles. The reason is that the standard **plot3d** command divided the given domain using a cartesian mesh, made of squares; this can be visualized when looking on the graph "from above", as shown in Figure 2b. Actually the plot is obtained using numerical computations: the CAS computes values of the function on the edges of the cells and make interpolations for what happens inside the cells, as explained in [2]. Zooming is useless, as this only inflates the cells, but does not compute new values for the function inside each cell.

Based on a prior mathematical analysis of the continuity of the function, a more accurate plot may be achieved using a new coordinate systems (See the reference [4]).

We choose new coordinates, which fit the specific coordinates of the given function. Figure 3a shows a plot of the function defined in Equation (1), using polar coordinates, with $x = r\cos\theta,\ y = r\sin\theta$. Even the choice of these coordinates do not ensure that the plot will be really accurate. Figure 3b and Figure 3c represent the same plot, viewed from different directions, after a slight modification of the domain. Here the interpolations once again hide the actual discontinuities.

Other modifications, such as considering $g(x,y) = 1/(3-(x^2+y^2))$, or $h(x,y) = 1/(1-(x^2+3y^2))$ lead students to understand the need for a mathematical analysis of the data prior to computerized work.

Algorithms have been described in [3] in order for the software to determine a mesh which will provide an accurate plot. In our talk we will present both further advances in this field, and actual situations encountered in classroom. Moreover, we



(a) $0 \leq r \leq 2,\ 0 \leq \theta \leq 2\pi$

(b) $0 \leq r \leq 3,\ 0 \leq \theta \leq 2\pi$

(c) $0 \leq r \leq 3,\ 0 \leq \theta \leq 2\pi$

Figure 3: The influence of the choice of the plotting domain

can mention the possibility to enhance more understanding by using Virtual Reality, as described in [1].

Keywords: surface, accurate plot, mesh

References

[1] Th. Dana-Picard; Y. Badihi; D. Zeitoun, *A new kind of representation in Multivariable Calculus: Mathematics learning assisted by Virtual Reality*, Preprint, Jerusalem (2017).

[2] D. Zeitoun; Th. Dana-Picard, Accurate visualization of graphs of functions of two real variables, *International Journal of Computational and Mathematical Sciences* 4(1), 1–11 (2010)

[3] D. Zeitoun; Th. Dana-Picard, Zooming algorithms for accurate plotting of functions of two real variables, in I.S. Kotsireas and E. Martínez-Moro (edts), *Applications of Computer Algebra 2015: Kalamata, Greece, July 2015*', Springer Proceedings in Mathematics & Statistics (PROMS Vol. 198), 499–515 (2017).

[4] D. Zeitoun; Th. Dana-Picard, On the usage of different coordinate systems for 3D plots of functions of two real variables, in Th. Dana-Picard, I.KOtsireas and A. Naiman (edts) *ACA 2017 Book of Abstracts*, 236–237 (2017), available: http://homedir.jct.ac.il/ naiman/aca2017/abstracts.eps. Extended paper submitted.

[1]Mathematics Department
Orot College of Education
Rehovot
Israel
ed.technologie@gmail.com

[2]Department of Mathematics
Jerusalem College of Technology
Havaad Haleumi St. 21
Jerusalem 9116011
Israel
ndp@jct.ac.il

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Addressing discrete mathematics problems in the classroom

A. Bergeron-Brlek[1]

The TI-Nspire CX CAS calculator is mandatory in all mathematics courses at École de technologie supérieure. Every student has a handheld device in the classroom and can use it in real time. Making students work actively in the classroom is an effective way for improving their knowledge and understanding of the concepts.

The compulsory course Logic and Discrete Mathematics (MAT210) is given to software engineering students. Using a CAS in this course enables the teacher and the students to explore more complex examples. For instance, students can manipulate large prime numbers in the study of the RSA cryptographic system, or solve recurrence relations related to counting problems. We study, among other topics in this course, the complexity of algorithms.

In this talk, we will present our approach to handle this notion. Using Nspire, students are guided in the implementation of several algorithms to solve the same problem. In order to measure the time complexity (using the big-O notation), they run the algorithms on samples of different size and plot the results. This leads to a better understanding of the big-O notation, which is then confirmed algebraically using the handheld device.

References

[1] K. ROSEN, *Discrete Mathematics and Its Applications*. McGraw-Hill, New York, 2012.

[1]Senior lecturer, Service des enseignements généraux
École de technologie supérieure, Université du Québec
1100 Rue Notre-Dame Ouest, Montréal, QC H3C 1K3
anouk.bergeron-brlek@etsmtl.ca

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Analyzing discrete suspended chains using computer algebra

Gilbert Labelle[1]

The mathematical description of the shape of various kinds of suspended chains, cables or funiculars under gravity is well covered in the scientific literature. In this talk we apply computer algebra to analyze, classify and animate suspended discrete chains whose links are "thin straight rods" joining the origin O to a variable endpoint P in the closed right half-plane. We use Lagrange multipliers to minimize the potential energy of each chain.

In contrast with the continuous limiting case of the catenary where the suspended chain is given explicitly (up to translation and zoom) as an arc of the hyperbolic cosine, the global shape of such discrete regular suspended chains has no simple explicit expression and falls into 3 classes :

Concave, Parallel, Convex,

according to the values of the Lagrange multipliers and the position of endpoint P. This provides to undergraduate students a stimulating example of the application of Lagrange multipliers and computer algebra methods to analyse a discrete optimization problem.

Keywords: Discrete chains, catenary, Lagrange multipliers, computer algebra

[1]Département de mathématiques / LaCIM
Université du Québec à Montréal (UQAM), Canada
C.P. 8888, Succ. Centre-Ville, Montréal (Québec) Canada H3C 3P8
labelle.gilbert@uqam.ca

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Consolidation of abstract knowledge in the process of confronting errors using digital tools: The case of the inflection point

Anatoli Kouropatov[1], **Regina Ovodenko**[2]

At the previous ACA conference (see the reference [6]) we reported the results about the development of the integrated teaching unit that was designed towards learning an entire mathematical concept – the inflection point. The unit was built in the digital environment ([3]]) and includes geogebra labs, interactive digital questionnaires, and videos, as well as a variety of investigative assignments that are based on them. This environment has been developed with special attention to addressing errors. The development of the environment was informed by research regarding the use of technological tools in math education and research about typical errors in specific mathematical subjects, such as functions ([2]), tangent lines ([1], [7], [9]), inflection ([8]), and so on. We theorized that learning with this unit would allow students to confront errors and to consolidate knowledge about the inflection point. With the purpose of testing this conjecture, we conducted a short feasibility study with a pair of first year students from the Industrial Engineering College. These students are considered advanced students (according to high formal achievements and their lecturer's personal opinion). It was suggested to the students that they learn the unit after they learned the concept of the inflection point during the course Calculus 1. Their previous encounter with this concept consisted of the part of the process that dealt with investigating functions based on algorithmical usage of well-known theorems related to the concept. The study was organized as a two-hour clinical interview in laboratory conditions. The students' work was documented and transcribed with the purpose of analyzing their learning process. The analysis of the students' learning process has been conducted using "Abstraction in Context" (AiC) as developed in [5] as a theoretical framework and as methodological tool ([4]). According to "Abstraction in Context", learners vertically reorganize previous elements of knowledge to construct new (for the learner) elements and to consolidate previously constructed (by the learner) elements. This construction/consolidation process takes place in students' minds in a specific context, in our case – learning the inflection point concept using the digital-based teaching unit. In the conference we will present the methodology we used at the study as well as empirical evidence regarding the students' learning process in general, and regarding the consolidation of abstract knowledge in the process of confronting errors using digital tools, in particular.

References

[1] M. ARTIGUE, The importance and limits of epistemological work in didactics. In *Proceedings of the 16th Conference of the International Group for the Psychology of Mathematics Education*, W. Geeslin, K. Graham (eds.),Vol.3, 195-216). Durham, NH: University of New Hampshire: PME..

[2] M. CARLSON, A cross-sectional investigation of the development of the function concept *Research in Collegiate Mathematics III, Issues in Mathematics Education*. **7**(2), 114-162.

[3] Challenge 5 (2016). Available at http://lo.cet.ac.il/player/?document=d6beaef0-48a8-4250-b42d-c98cfae422a6, CET, Israel, 2016.

[4] T. DREYFUS; R. HERSHKOWITZ; B. SCHWARZ, The nested epistemic actions model for abstraction in context - Theory as methodological tool and methodological tool as theory. In *Approaches to qualitative research in mathematics education: Examples of methodology and methods*, A. Bikner-Ahsbahs; C. Knipping; N. Presmeg (Eds.),185-217, Dordrecht, Springer: Advances in Mathematics Education Series. Ninth Edition, Pearson, 2018.

[5] R. HERSHKOWITZ; B. SCHWARZ; T. DREYFUS, Abstraction in context: epistemic actions. *Journal for Research in Mathematics Education*. **32**, 195-222.

[6] R. OVODENKO; A. KOUROPATOV, The use of digital tools to confront errors. In *Proceedings of 23rd Conference on Applications of Computer Algebra* . ACA 2017.

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

[8] P. TSAMIR; R. OVODENKO, University students' grasp of inflection points. *Educational Studies in Mathematics*. **83**, 409-427.

[9] S. VINNER, Conflicts between definitions and intuitions – the case of the tangent. In *Proceedings of the 6th International Conference for the Psychology of Mathematical Educations*, A. Vermandel (Ed.), 24-29. Antwerp, Belgium: PME.

[1]Center for Educational Technology and the Levinsky College of Education
Tel-Aviv, Israel
anatoliko@gmail.com

[2]Center for Educational Technology
Israel
ReginaO@cet.ac.il

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Periodic and Nontrivial Periodic Input in Linear ODEs (Part I, Part II)

Michel Beaudin[1]

Differential equations courses are among the ones where the use of computer algebra systems (CAS) was first experienced. In many cases. it was and it is still for solving application problems where the computation can become very long and tedious. Textbooks as [1] and [2] contain very interesting projects on which students can work. Unfortunately, some authors seem to forget the important role CAS can play in increasing student's understanding of theoretical concepts.

The first part of the talk will be devoted to introduce the subject: we will present the classical problem of finding the steady-state solution of a damped mass-spring problem where the external force is a pure cosine of different frequency. Then, in the second part, the external force will be a nontrivial periodic one. This is well documented but we rarely see different approaches. One approach we will use is the convolution of the input with the impulse response. Another approach will be the use of Fourier series because the linearity of the differential equation allows us to apply the principle of superposition. In both cases, the CAS will work for us, computing the convolution and finding the Fourier expansion.

Finally in the case of underdamping, the shape of the frequency response is best understood and illustrated with the aid of sliders. For this purpose, the TI-Nspire CX CAS software will be used. The notebook [3] contains many examples of how to use it in differential equations.

References

[1] R. KENT NAGLE; EDWARD B. SAFF; ARTHUR D. SNIDE, *Fundamental of Differential Equations*. Ninth Edition, Pearson, 2018.

[2] ERWIN KREYSZIG, *Advanced Engineering Mathematics*. Tenth Edition, John Wiley and Sons, 2011.

[3] GILLES PICARD, *Notes de cours MAT265, Équations différentielles*. Available at https://cours.etsmtl.ca/seg/gpicard/mat265V2.pdf, 2017.

[1]Senior lecturer, Service des enseignements généraux
École de technologie supérieure, Université du Québec
1100 Notre-Dame street West, Montréal, Québec, Canada, H3C 1K3
michel.beaudin@etsmtl.ca

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Introducing parametric curves with CAS

Louis-Xavier Proulx[1]

The TI-Nspire CX CAS handheld device is mandatory in every math courses at École de technologie supérieure. Our engineering students learn single-variable calculus in a one-term course (MAT145). Students get their motivation to learn mathematical concepts through applied problems. Hence, in-house course notes [1] were written to emphasize on the applications of the syllabus material and the use of CAS.

The multi-variable calculus course (MAT165) follows a classic reference textbook [2] contrary to the more hands-on approach pursued in MAT145. Many concepts can be explored and visualized with graphs of level surfaces. Plotting 3D objects is a useful feature of TI-Nspire, but it requires the use of parametric curves and surfaces. Vector functions are a fundamental tool for the course, but students hardly conciliate the graphical representations of these functions with their algebraic definition. Moreover, the students are challenged by the general and abstract setting in which these mathematical concepts are introduced.

The aim of this talk is to explore alternative ways for introducing the concept of parametric curves and vector functions using computer algebra. More focus will be given to different vector calculus concepts presented in applied problems. Software such as TI-Nspire will be used to graph and manipulate parametric curves.

Keywords: Parametric curves, Vector functions, Applications

References

[1] G. SAVARD, R. MICHAUD AND A. BORDELEAU, *MAT145 Calcul différentiel et intégral, notes de cours*, vol 1 and 2, 2017

[2] J. STEWART, *Concepts et contextes, Fonctions de plusieurs variables*, De Boeck, 2011

[1]Senior Lecturer, Service des enseignements généraux
École de technologie supérieure, Université du Québec
1100 rue Notre-Dame Ouest, Montréal, Québec, Canada, H3C 1K3
louis-xavier.proulx@etsmtl.ca

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Visualizations of the nondominated set and the efficient set in multicriteria optimization problems using Mathematica

Włodzimierz Wojas[1], **Jan Krupa**[1]

Multicriteria optimization also known as multicriteria programming is a subdiscipline of operation research. It is taught students in framework of such academic courses as for example: Operation research, Multiobjective optimization, Optimization methods or Mathematical programming. Multicriteria optimization problem has a general form:

$$f(x) = (f_1(x), f_2(x), \ldots, f_k(x)) \to \text{min/max}$$
$$\text{subject to } x \in X, X \subset \mathbb{R}^n$$

where x is a decision variable vector, X is a feasible set in decision space $\mathbb{R}^n$, $(f_1(x), f_2(x), \ldots, f_k(x))$ is a criterion vector and min or max are understood in accordance with the partial order P in criterion space $\mathbb{R}^k$. We define: a feasible set Y in criterion space as the image of the set X under $f = (f_1, f_2, \ldots, f_k)$, the nondominated set $Y_N = \{y \in Y : \text{there is not } y' \in Y \text{ with } y'Py\}$ and the efficient set $X_E = \{x \in X : f(x) \in Y_N\}$. Many academic books contain visualizations of sets X, Y, Y_N, X_E for some linear functions $f : \mathbb{R}^2 \to \mathbb{R}^2$. It would be more difficult but didactically useful to present these sets also for functions $f : \mathbb{R}^2 \to \mathbb{R}^3$ and $f : \mathbb{R}^3 \to R^3$. It would rather require computer support using for example CAS programs. In this talk we would like to present a few didactic visualizations of sets X, Y, Y_N, X_E for some functions $f : \mathbb{R}^2 \to \mathbb{R}^3$ and $f : \mathbb{R}^3 \to \mathbb{R}^3$ using Mathematica.

Keywords: multicriteria optimization, multicriteria programming, didactics of mathematics, mathematics education, CAS, Mathematica

References

[1] RENATA DUDZIŃSKA-BARYŁA, DONATA KOPAŃSKA-BRÓDKA, EWA MICHALSKA, *Software tools in didactics of mathematics*, DIDACTICS OF MATHEMATICS, No. 12 (16) 2015

[2] R.E. STEUER, *Multiple criteria optimization: theory, computation, and application*, Wiley (1986)

[3] M. EHRGOTT, *Multicriteria optimization*, Springer (2005)

[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)

[1]Department of Applied Mathematics
Warsaw University of Life Sciences (SGGW)
Warsaw Poland
wlodzimierz_wojas@sggw.pl
jan_krupa@sggw.pl

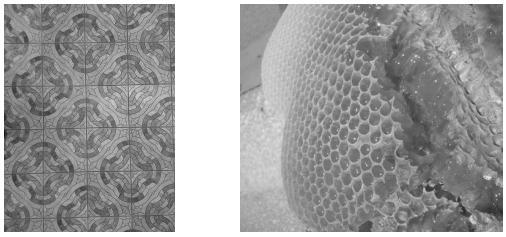
Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Fractals and tessellations: from K's to cosmology

Thierry Dana-Picard[1], **Sara Hershkovitz**[2]

We present two related topics which can accompany Mathematics Education from early childhood to university and even beyond.

1. A *tessellation* is a partition of a space (usually a Euclidean space like the Euclidean plane or the Euclidean 3-dimensional space) by elements of a finite set, called tiles (more precisely, they are non-empty compacts). We begin with considering tilings by translations, i.e. two isometric tiles are deductible from one another by a translation (excluding rotations or symmetries). Generalization is possible to surfaces locally topologically equivalent to a plane. See Figure 1. Another generalization is to accept symmetries (either central or axial), as the



(a) Plane tessellation

(b) Honeycomb

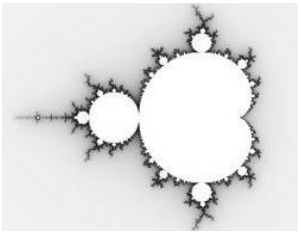
Figure 1: Tessellations

tessellation using a 4^{th} generation Sierpinski triangle in Figure 3 (b).

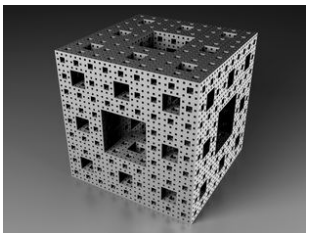
2. A *fractal* is an abstract object used to describe and simulate naturally occurring objects, showing self-similarity at increasingly small scales. Among the most known examples is the *Mandelbrot set* (Figure 1 (a)). An example of a 3D fractal is the so-called *Menger sponge*. See Figure 2

We show how to use a standard triangular grid to produce tessellation, and how to use a fractal to build a tessellation. Figure 3 shows a Sierpinski triangle, a plane tessellation built with it and a Sierpinski pyramid.

Different levels of technology can be used: low-tech such as paper and pencil, then progressive introduction of Dynamic Geometry (in our case GeoGebra: `http://geogebra.org`) and Computer Algebra Systems (we used Maple 2017), together with easy free software to work with images (Irfanview: `http://irfanview.com`).

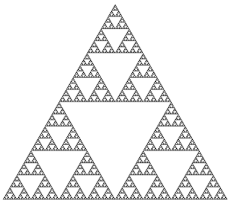


(a) Mandelbrot set

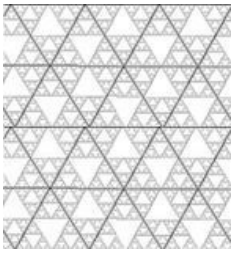


(b) Menger sponge

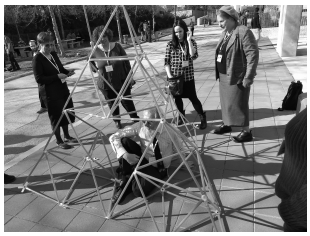
Figure 2: 2D and 3D fractals



(a) Sierpinski triangle



(b) Sierpinski tessellation



(c) Sierpinski pyramid

Figure 3: 2D and 3D fractals

We demonstrate how to work with technology, using GeoGebra applets, animations* and Maple programming. The examples serving as a basis can come from everyday life and also from more advanced scientific topics, such as the shape of space. In particular, we may quote the following works:

> [(i)]Luminet's theory of *wrapped universe* [1] relies on a kind of 3D tessellation; see Figure 4 (a). A work presented at ACA 2017 in Jerusalem in the session on Applied Physics [2], describing the repartitions of galaxies using a Sierpinski gasket; see Figures 4 (b) and (c)†.

Part of this exploration has been performed with in-service teachers in a special lab, last February.

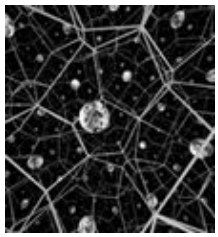
Keywords: Tessellations, Fractals, CAS, DGS

References

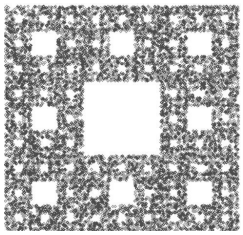
[1] J.P. LUMINET, *The wraparound Universe*. AK Peters, 2008.

*such as `https://www87.homepage.villanova.edu/richard.hurst/Sierpinski.htm\#Sierpinski_Carpet`

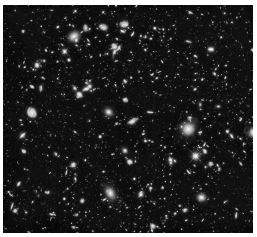
†Credit: NASA/Hubble



(a) Wraparound universe



(b) Sierpinski gasket



(c) Repartition of galaxies

Figure 4: The shape of space

[2] J. BENJAMIN; D. WALKER; A. MYLLÄRI AND T.MYLL, On the Applicability of Pairwise Separations Method in Astronomy: Influence of the Noise in Data. In *ACA 2017 Book of Abstracts*, Th. Dana-Picard, I. Kotsireas and A. Naiman (eds.), 142–144. JCT, Jerusalem, 2017. Avalaible: `http://homedir.jct.ac.il/~naiman/aca2017/abstracts.pdf`.

[1]Department of Mathematics
Jerusalem College of Technology
Havaad Haleumi St. 21, Jerusalem, Israel
`ndp@jct.ac.il`

[2]Center for Educational Technology
Klausner St., 16
Tel Aviv, Israel
`sarah@cet.ac.il`

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

The Runge Example for Interpolation and Wilkinson's Examples for Rootfinding

Leili Rafiee Sevyeri[1], **Robert M. Corless**[2]

We look at two classical examples in the theory of numerical analysis, namely the Runge example for interpolation and Wilkinson's example (actually two examples) for rootfinding. We use the modern theory of backward error analysis and conditioning, as instigated and popularized by Wilkinson, but refined by Farouki and Rajan. By this means, we arrive at a satisfactory explanation of the puzzling phenomena encountered by students when they try to fit polynomials to numerical data, or when they try to use numerical rootfinding to find polynomial zeros. Computer algebra, with its controlled, arbitrary precision, plays an important didactic role.

Keywords: Interpolation, Rootfinding, Conditioning, Sensitivity.

References

[1] CORLESS, ROBERT M.; FILLION, NICOLAS, *A Graduate Introduction to Numerical Methods: from the Viewpoint of Backward Error Analysis*. Springer Publishing Company, Incorporated, 2013.

[2] TREFETHEN, LLOYD N., *Approximation theory and approximation practice*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2013.

[3] FAROUKI, R; RAJAN, VT, On the numerical condition of polynomials in Bernstein form. *Computer Aided Geometric Design* **volumen**(4-3), 191–216 (1987).

[4] FAROUKI, R; GOODMAN, T, On the optimal stability of the Bernstein basis. *Mathematics of Computation of the American Mathematical Society* **volumen**(65-216), 1553–1566 (1996).

[5] J.M. CARNICER; Y. KHIAR; J.M. PEÑA, Optimal stability of the Lagrange formula and conditioning of the Newton formula. *Journal of Approximation Theory* (2017).

[6] WILKINSON, JAMES H., The perfidious polynomial. *MAA Stud. Math.* **volumen**(24), 1–28 (1984).

[7] KIRK GREEN; THOMAS WAGENKNECHT, Pseudospectra and delay differential equations. *Journal of Computational and Applied Mathematics* **volumen**(196-2), 567–578 (2006).

[8] AMIRASLANI, A, New Algorithms for Matrices, Polynomials and Matrix Polynomials. *PhD thesis, Western University*, (2006).

[9] BECKERMANN, BERNHARD, The condition number of real Vandermonde, Krylov and positive definite Hankel matrices. *Numerische Mathematik* **volumen**(85-4), 553–577 (2000).

[10] ROBERT M. CORLESS; STEPHEN M. WATT, Bernstein bases are optimal, but, sometimes, Lagrange bases are better. *In Proceedings of SYNASC, Timisoara*, 141–153. MIRTON Press, 2004.

[1]Ontario Research Center for Computer Algebra and The School of Mathematical and Statistical Sciences.
University of Western Ontario
lrafiees@uwo.ca

[2]Ontario Research Center for Computer Algebra and The School of Mathematical and Statistical Sciences.
University of Western Ontario
rcorless@uwo.ca

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

A non-iterative method for solving nonlinear equations

Michael Xue[1]

Newton-Raphson method is the most commonly used iterative method for finding the root(s) of a real-valued function or nonlinear systems of equations. However, its convergence is often sensitive to the error in its initial estimation of the root(s). This talk will present a non-iterative method that mitigates non-convergence. An auxiliary initial-value problem of ordinary differential equation(s) is generated by a Computer Algebra System first, then integrated numerically over a closed interval. The solution(s) to the original systems of nonlinear equations is obtained non-iteratively at the end of the interval. A proof of the theorem serving as the base for this new method is presented at the talk. Several examples will illustrate its guaranteed convergence, a clear advantage over the Newton-Raphson method.

Keywords: Non-iterative method, Convergence, Nonlinear equations, Computer algebra

References

[1] P. HENRICI, *Elements of Numerical Analysis*. John Wiley & Sons Inc. 1964

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

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

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

What is the integral of x^n ?

David J. Jeffrey[1], **David R. Stoutemyer**[2] **Robert M. Corless**[1]

Thus, computer algebra systems usually solve a problem under the implied assumption that any parameters appearing in the problem will take values that lead to the general result returned. The title refers to the fact that the systems return the integral of x^n as $x^{n+1}/(n+1)$ while omitting the condition $n \neq -1$.

We shall use the word *specialization* to describe the action of substituting specific values (usually numerical, but not necessarily) into a formula. The *specialization problem* is a label for a cluster of problems associated with formulae and their specializations, the problems ranging from inelegant results to invalid ones. For example, in [2] an example is given in which the evaluation of an integral by specializing a general formula misses a particular case for which a more elegant expression is possible. The focus here, however, is on situations in which specialization leads to invalid or incorrect results. To illustrate the problems, consider

$$I_1 = \int \left(\alpha^{\sigma z} - \alpha^{\lambda z}\right)^2 dz = \frac{1}{2\ln\alpha}\left(\frac{\alpha^{2\lambda z}}{\lambda} + \frac{\alpha^{2\sigma z}}{\sigma} - \frac{4\alpha^{(\lambda+\sigma)z}}{\lambda+\sigma}\right). \qquad (1)$$

Expressions equivalent to this are returned by Maple, Mathematica and many other systems, such as the Matlab symbolic toolbox. It is easy to see that the specialization $\sigma = 0$ leaves the integrand in (1) well defined, but the expression for its integral on the right-hand side is no longer defined. If we pursue this further, we see that there are multiple specializations for which (1) fails, *viz.* $\alpha = 0$, $\alpha = 1$, $\lambda = 0$, $\sigma = 0$, $\lambda = -\sigma$, and combinations of these. The question of how or whether to inform computer users of these special cases has been discussed in the CAS literature many

times [1]. A list of every special case for (1) is as follows.

$$I_1 = \begin{cases} \dfrac{1}{2\lambda \ln \alpha}\left(\alpha^{2\lambda z} - \alpha^{-2\lambda z} - 4z\lambda \ln \alpha\right) , & \left[\begin{array}{l} \lambda + \sigma = 0 , \\ \alpha \neq 0 , \alpha \neq 1 , \sigma \neq 0 ; \end{array}\right. \\ z + \dfrac{1}{2\lambda \ln \alpha}\left(\alpha^{\lambda z}(\alpha^{\lambda z} - 4)\right) , & \left[\begin{array}{l} \sigma = 0 , \\ \alpha \neq 0 , \alpha \neq 1 , \lambda \neq 0 ; \end{array}\right. \\ z + \dfrac{1}{2\sigma \ln \alpha}\left(\alpha^{\sigma z}(\alpha^{\sigma z} - 4)\right) , & \left[\begin{array}{l} \lambda = 0 , \\ \alpha \neq 0 , \alpha \neq 1 , \sigma \neq 0 ; \end{array}\right. \\ \text{ComplexInfinity} , & \left[\begin{array}{l} \alpha = 0 , \\ \Re(\lambda z)\,\Re(\sigma z) < 0 ; \end{array}\right. \\ \text{Indeterminate} , & \left[\begin{array}{l} \alpha = 0 , \\ \Re(\sigma z)\,\Re(\lambda z) \geq 0 ; \end{array}\right. \\ \dfrac{1}{2\ln \alpha}\left(\dfrac{\alpha^{2\lambda z}}{\lambda} + \dfrac{\alpha^{2\sigma z}}{\sigma} - \dfrac{4\alpha^{(\lambda+\sigma)z}}{\lambda+\sigma}\right) , & \text{otherwise, (generic case)} . \end{cases} \tag{2}$$

Expressions such as this will be called *comprehensive antiderivatives*. There are several questions surrounding such expressions. The first is whether comprehensive antiderivatives should be returned to users. A second question is how systems can compute such expressions. The automatic discovery of exceptional cases is not easy. A third question concerns *continuity with respect to parameters.*

We shall discuss why the expression

$$\int x^n \, dx = \frac{x^{n+1}}{n+1} - \frac{1}{n+1}$$

is better than the usual expression, and how we found it.

Keywords: Specialization problem, integration, parameters, continuity

References

[1] R. M. CORLESS; D. J. JEFFREY, *Well... it isn't quite that simple*. *SIGSAM Bulletin* **26**(3), 2–6 (1992).

[2] D. J. JEFFREY; A.D. RICH, Reducing expression size using rule-based integration. *Intelligent Computer Mathematics*, Editor: S. Autexier, LNAI6167, 234–246, Springer (2010)

[1]Department of Applied Mathematics, and ORCCA
University of Western Ontario
London, Ontario, Canada
djeffrey, rcorless@uwo.ca

[2]University of Hawaii
Honolulu, HI, USA
dstout@hawaii.edu

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

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

Włodzimierz Wojas[1], **Jan Krupa**[1], **Jarosław Bojarski**[1]

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

In this talk we present some examples of calculation the Lebesgue measure of some subsets of $\mathbb{R}^2$ directly from definition. We cannot find such examples in the literature we know. We will consider the following subsets of $\mathbb{R}^2$: $\{(x,y) \in \mathbb{R}^2 : 0 \leq y \leq x^2, 0 \leq x \leq 1\}$, $\{(x,y) \in \mathbb{R}^2 : 0 \leq y \leq \sin x, 0 \leq x \leq \pi/2\}$, $\{(x,y) \in \mathbb{R}^2 : 0 \leq y \leq \exp(x), 0 \leq x \leq 1\}$, $\{(x,y) \in \mathbb{R}^2 : 0 \leq y \leq \ln(1-2r\cos x+r^2), 0 \leq x \leq \pi\}$, $r > 1$. The aim of these examples is to familiarize students with the definition of Lebesgue measure. We calculate sums, limits and plot graphs and dynamic plots of needed sets and unions of rectangles sums of which volumes approximate Lebesgue measure of the sets, using Mathematica. The title of this talk is very similar to the title of author's article [1] which deals with definition of Lebesgue integral but our talk deals with definition of Lebesgue measure instead. Using Mathematica or others CAS programs for calculation Lebesgue measure directly from its definitions, seems to be didactically useful for students because of the possibility of symbolic calculation of sums, limits - checking our hand calculations and plot dynamic graphs. Moreover we get students used not only to definition of Lebesgue measure but also to CAS applications generally.

The following definitions we will use in our talk (see [9, 3]):

Rectangles. A closed rectangle R in $\mathbb{R}^d$ is given by the product of d one-dimensional closed and bounded intervals: $R = [a_1, b_1] \times [a_2, b_2] \times \cdots \times [a_d, b_d]$, where $a_j \leq b_j$ are real numbers, $j = 1, 2, \ldots, d$. In other words, we have $R = \{(x_1, \ldots, x_d) \in \mathbb{R}^d : a_j \leq x_j \leq b_j \text{ for all } j = 1, 2, \ldots, d\}$. We remark that in our definition, a rectangle is closed and has sides parallel to the coordinate axis. In $\mathbb{R}$, the rectangles are precisely the closed and bounded intervals, while in $\mathbb{R}^2$ they are the usual four-sided rectangles. In $\mathbb{R}^3$ they are the closed parallelepipeds.

We say that the lengths of the sides of the rectangle R are $b_1 - a_1, \ldots, b_d - a_d$. The volume of the rectangle R is denoted by $\mathrm{vol}\,(R)$, and is defined to be $\mathrm{vol}\,(R) = (b_1 - a_1) \cdots (b_d - a_d)$.

Definition 1. (see [3, 7, 8, 9]) Let $(\mathbb{R}^2, \mathfrak{M}, m)$ be measure space, where $\mathfrak{M}$ is $\sigma-$ algebra of Lebesgue measurable subsets in $\mathbb{R}^2$, and m- Lebesgue measure on $\mathbb{R}^2$.

The measure m for any $A \in \mathfrak{M}$ is defined by the following formula:

$$m(A) = \inf \Big\{ \sum_{j=1}^{\infty} \mathrm{vol}\,(R_j) : A \subset \bigcup_{j=1}^{\infty} R_j, \quad R_j \ \text{ is closed rectangle in } \mathbb{R}^2, j \in \mathbb{N} \Big\}. \tag{1}$$

Keywords: Higher education, Lebesgue measure, Application of CAS, Mathematica, Mathematical didactics

References

[1] WŁODZIMIERZ WOJAS AND JAN KRUPA, Familiarizing Students with Definition of Lebesgue Integral: Examples of Calculation Directly from Its Definition Using Mathematica, *Mathematics in Computer Science*, **11**, 363–381, http://doi.org/10.1007/s11786-017-0321-5, (2017)

[2] CHARALAMBOS D. ALIPRANTIS, OWEN BURKINSHAW, *Principles of Real Analysis*, 3rd ed., Academic Press, (1998)

[3] ROBERT G. BARTLE, *The Elements of Integration and Lebesgue Measure*, Wiley-Interscience, (1995)

[4] FRANK JONES, *Lebesgue Integration On Euclidean Space*, Jones & Bartlett Learning, (2000)

[5] ANDREW BROWDER, *Mathematical Analysis An Introduction*, 2nd ed., Springer, (2001)

[6] GERALD B. FOLLAND, *Real Analysis Modern Technique*, 2nd ed., Wiley, (2007)

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

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

[9] ELIAS M. STEIN, RAMI SHAKARCHI, *Real Analysis: Measure Theory, Integration, and Hilbert Spaces*, Princeton University Press, (2003)

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

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

[1]Department of Applied Mathematics
Warsaw University of Life Sciences (SGGW)
Warsaw Poland
wlodzimierz_wojas@sggw.pl
jan_krupa@sggw.pl
jaroslaw_bojarski@sggw.pl

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

CAS in Teaching Basics of Stereoscopy

Jurell Benjamin[1], **Donna Walker**[1], **Mylläri Tatiana**[1], **Mylläri Aleksandr**[1]

We use Wolfram Mathematica in teaching the basics of stereoscopy. Each stereo image is represented either as a stereopair (for parallel and cross-eye views) or as an anaglyph image (to be viewed with red-cyan glasses). By changing the parallax of the left and right parts of the stereogram, one can move the image (or some part of it) in front of or behind the window frame. We demonstrate basic stereoscopic effects and typical mistakes made by beginners.

Soon after the invention of photography in 1839, a first suggestion for a stereo camera was given by Brewster in 1847. By 1860 viewing stereo photos was a popular pastime [1]. Later - in 20th century - interest waned. Recently, with the development of technology interest in 3D imaging has increased: 3D cameras are available; 3D lenses exist for cameras and smartphones; 3D cartoons and movies can be watched on an ordinary tv or computer screen using anaglyph (red-cyan) glasses; there are special 3D TVs, 3D movie cinemas, glasses-free 3D displays, etc.; and, finally, the recent development of virtual reality.

Here, we demonstrate some basic tricks one can do with changing the position of the stereo window and basic mistakes of beginners (and not only beginners - similar mistakes can be seen in big-screen, multi-million-dollar budget movies!). For example, one of the standard "Wow!" effects with 3D images is when most of the image appears behind the frame, but part of the image is hanging out in front. One has to be careful: that part shouldn't be cut by the frame! It is especially important in action scenes when objects which are moving around can easily be cut by the frame border.

Wolfram Mathematica provides good tools for image processing as well as powerful analytic tools, 3D graphics and animation. These allow one to easily construct simple stereograms; demonstrate effects and distortions introduced by the incorrect methods of constructing stereo image; and manipulate constructed images to demonstrate different effects. We use Mathematica to demonstrate correct and incorrect "Wow!" effect realizations of the type described above. By changing relative parallax of left and right images, we change position of the image with respect to the frame. Our manipulations with stereo images we base on a classic textbook by J.G. Ferwerda [1].

Keywords: Stereoscopy, 3D Imaging

References

[1] J.G. FERWERDA, *The World Of 3-D: A Practical Guide To Stereo Photography* . 3-D Production, 2003.

[1]Dept. of Computers & Technology, SAS
St.George's University
St.George's, Grenada, West Indies
jbenjam2@sgu.edu

S4
Applied Computational Algebraic Topology

Algebraic Topology was in its origin an area of pure mathematics with deep algebraic and geometrical roots, which has had an intense development in the last 120 years. However, in this period this discipline has become the core of several areas of application-oriented research using algebraic topology methods in biology, statistics, engineering, computer science... The growing number of these interactions has given rise to the field of applied and computational algebraic topology.

This session is therefore mainly devoted to the computational aspects of this emerging field in all possible directions which include, but are not restricted to:

- Computational algebraic topology
- Computational homological algebra
- Computational topological dynamics
- Coding theory and cohomology of groups
- Topological analysis and processing of digital images
- Topological analysis of data
- Stochastic algebraic topology
- Topological pattern recognition
- Topological robotics
- Topology, computer science and parallelism

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

New algorithms for computing homology of finite topological spaces

Julián Cuevas-Rozo[1], **Laureano Lambán**[2], **Ana Romero**[2], **Humberto Sarria Zapata**[1]

We present some algorithms to compute the homology of finite topological spaces, which have been implemented in the Kenzo system by combining techniques of point reduction of finite topologies and discrete vector fields.

Keywords: Finite topological space, simplicial complex, discrete vector field, homology.

1 Introduction

A useful correspondence between finite topological spaces and finite simplicial complexes is due to McCord [6], who assigns to each finite T_0 space X a simplicial complex $\mathcal{K}(X)$, called the *order complex of* X, in such a way that X and $\mathcal{K}(X)$ are weak homotopy equivalent. In addition, McCord proves that weak homotopy types of compact polyhedra are in one-to-one correspondence with those of finite topological spaces.

In the last years the theory of finite topological spaces has experimented a new impulse from works by Barmak and Minian [2] about the study of homotopy and weak homotopy types, among many other results; for example, they show that elementary collapses of compact polyhedra correspond to elimination of *weak points* of finite T_0-spaces. On the other hand, Minian [7] introduced a version of discrete Morse theory for posets that satisfy the *h-regularity* property; the incidence graphs of simplicial complexes are *h-regular* so that Minian's results apply to any finite topological space coming from the simplicial context.

More recently, Cianci and Ottina [3] have generalized Minian's results by defining an appropriate spectral sequence that converges to the homology of a finite T_0-space and showing that, in the particular case of *quasicellular posets*, the computation is more tractable. In this work we present the implementation of some algorithms in the Kenzo system [5] to compute topologial invariants of finite spaces. The Kenzo system was developed by Francis Sergeraert and some coworkers and it allows the user to compute homotopy and homology invariants of spaces by using their simplicial versions. Our algorithms combine theoretical results by Barmak and Minian and some previous ideas implemented in Kenzo, as the technique of discrete vector fields.

2 Computation of homology in finite spaces

Given a finite T_0-space $(X, \mathcal{T})$ where $X = \{x_1, \ldots, x_n\}$, the *topogenous matrix* associated to X is the n-square matrix $T_X = [t_{ij}]$ defined by

$$t_{ij} = \begin{cases} 1 & , x_i \in U_j \\ 0 & , x_i \notin U_j \end{cases}$$

where U_j is the minimal open set that contains x_j. There exists a well-known result due to Alexandroff [1] providing a one-to-one correspondence between finite topological spaces and posets (the order relation is given by: $x_i \leqslant x_j \longleftrightarrow x_i \in U_j$). In this way, the topogenous matrix can be regarded as the incidence matrix corresponding to the order relation and U_x is the set of elements that are less than or equal to x. Moreover, in the previous work [4] it is shown how to modify T_X in order to obtain an upper triangular permutation-similar matrix, such that it is associated to a T_0-space which is homotopically equivalent to X. For this reason, we assume that a finite T_0-space X has an enumeration of its elements in such a way that its topogenous matrix is upper triangular. Usually a poset is represented by its Hasse diagram $\mathcal{H}(X)$, given by edges (x, y) such that $x < y$ and there does not exist z such that $x < z < y$.

If X is a finite T_0-space, the *order complex* $\mathcal{K}(X)$ associated to X is the simplicial complex whose simplices are the nonempty chains of X. The simplicial complex $\mathcal{K}(X)$ can be used to compute the topological invariants of X; the problem is the size of $\mathcal{K}(X)$, which limits the possible computations on it. In fact, the McCord morphism [6] provides a weak homotopy equivalence between X and $\mathcal{K}(X)$. Nevertheless, there exist methods that can be directly apply to finite spaces. For instance, Stong [9] proved that by sequencially removing some particular points in a finite T_0-space X, a minimal space, which is homotopy equivalent to X, is obtained; this space is called a *core* of X. Moreover, to decide if two spaces have the same homotopy type is equivalent to verify that their cores are homeomorphic.

With regard to homology, some results given in [2], [7] can help us to develop algorithms for computing homology groups of some particular classes of finite topological spaces. A space X is called *h-regular* if for every $x \in X$, the order complex $\mathcal{K}(\hat{U}_x)$ is homotopy equivalent to the sphere S^{n-1}, where n is the *degree* of x, that is, the maximum of the cardinality of the chains of $\hat{U}_x$ ($\hat{U}_x$ denotes the subspace $U_x - \{x\}$ in the poset associated to X). In the same way, a *cellular* poset X is a graded poset such that for every $x \in X$, $\hat{U}_x$ has the homology of S^{n-1}, where n is the degree of x.

We say that an edge (x, y) in the Hasse diagram $\mathcal{H}(X)$ is *admissible* if the subposet $\hat{U}_y - \{x\}$ is homotopically trivial. A poset is *admissible* if all its edges are admissible. It can be proved that any admissible poset is h-regular and the face poset $\mathcal{X}(K)$ (the poset given by the simplices of K ordered by subset inclusion) of any regular CW-complex K (in particular, of any finite simplicial complex) is admissible.

Given a cellular poset X, its *cellular chain complex* (C_*, d) is defined in [7] by

$$C_p(X) = \bigoplus_{\deg(x)=p} H_{p-1}(\hat{U}_x) \tag{1}$$

where $H_k(Y)$ denotes the k-homology group of Y.

Then, the following result [7, Theorem 3.7] provides a framework to compute homology.

Theorem 1. Let X be a cellular poset and let (C_*, d) be its cellular chain complex. Then $H_*(C_*) = H_*(X)$.

In order to improve the efficiency, one can consider discrete vector fields, a basic tool in homology computations. Let X be an h-regular poset and let $\mathcal{H}(X)$ be its Hasse diagram. A matching M is a *Morse matching* provided that the directed graph $\mathcal{H}(X)$ is acyclic and M is called *admissible* if all its edges are admissible. Corollary 3.15 in [7] asserts that the homology of a cellular poset X coincides with the homology of a complex $(\bar{C}_*, \bar{d})$, obtained by restricting only to those direct summands of (1) corresponding to the set C_M of critical points of M (those points that are not incident to any edge in M).

Theorem 2. Let X be a cellular poset with an admissible Morse matching M defined on it. Then $H_*(\bar{C}_*) = H_*(X)$, where $(\bar{C}_*, \bar{d})$ is defined by

$$\bar{C}_p(X) = \bigoplus_{\substack{\deg(x)=p \\ x \in C_M}} H_{p-1}(\hat{U}_x). \tag{2}$$

3 New algorithms and its implementation

In this section we are going to present some algorithms developed in Kenzo allowing the user to make topological computations over finite spaces. In particular, we provide algorithms to determine the core and the order complex of a space X. Moreover, we present an ongoing work for the computation of homology groups by using discrete vector fields.

An element x is a *beat point* of the space X if either $\hat{U}_x$ has a maximum or the set $\{y \in X : x < y\}$ has a minimum. A *core* of a finite T_0-space X is a strong deformation retract of X which has no beat points; in [9] it is proved that the core can be obtained by removing one by one all the beat points of X.

Given an element $x_k \in X$, we have implemented an algorithm to decide if x_k is a beat point by using the topogenous matrix $T_X = [t_{ij}]$ as follows: consider the sets $I_k = \{i : t_{ik} = 1, i \neq k\}$ and $J_k = \{j : t_{kj} = 1, j \neq k\}$ and the numbers $M_k = \max I_k$, $m_k = \min J_k$; if either $I_k = \{i : t_{i,M_k} = 1\}$ or $J_k = \{i : t_{m_k,j} = 1\}$ then x_k is a beat point. Once we know that x_k is a beat point, we can delete the k-th row and column in order to obtain a smaller topogenous matrix that represents the space $X - \{x_k\}$; continuing this process, after a finite number of steps, we will have the topogenous matrix of a core of X.

In [2] another kind of points that preserves the weak homotopy type is defined; these points are called *weak points* and satisfy the following property: x is a weak point if the link of x (the subspace consisting of all the elements comparable with x, different to x) is contractible. Since the algorithm to find the core of a space is already implemented, we have a procedure to decide if x_k is a weak point: consider the set $L_k = \{l \neq k : t_{lk} = 1 \text{ or } t_{kl} = 1\}$ and delete the r-th row and column from T_X for all $r \notin L_k$ in order to obtain the topogenous matrix $T_{\hat{C}_{x_k}}$ of the link; then, the matrix of the core of this link has size 1 if and only if x_k is a weak point.

We can also compute the order complex of any finite topology making use of its topogenous matrix. More exactly, if we consider the matrix N_T obtained from T_X by substracting the identity matrix i.e. $N_T = T_X - \mathbb{I}_n$, we have the following proposition.

Proposition. [4] For each $0 \leqslant k \leqslant n-1$, the entry $[N_T^k]_{ij}$ represents the number of chains of $k+1$ elements with x_i as minimum and x_j as maximum.

The above result allows us to find all the chains of elements in X from the successive powers of N_T, and therefore Kenzo is able to compute the order complex of a finite space.

With regard to homology, in order to define an admissible Morse matching on $\mathcal{H}(X)$, we have modified the algorithm proposed in [8, Section 5.2] (for computing admissible discrete vector fields for digital images), with the purpose it can be applied to any cellular space. In addition, the involved calculations to verify the cellularity condition improve the efficiency by means of the sequential construction of the discrete vector field. At first instance, we consider those edges (x, y) where the core of $\hat{U}_x - \{y\}$ is a single point (in this case, $\hat{U}_x - \{y\}$ is contractible), which is a stronger condition than being homotopically trivial, and combine this with the modified algorithm in [8] in order to obtain admissible vectors up to degree $p-1$. Then, we can compute all the homology groups $H_{p-1}(\hat{U}_x)$ appearing in (2) by applying Theorem 2 to $X := \hat{U}_x$ together with those vectors contained in it. In this manner, the Kenzo system uses in a recursive way Theorem 2 and the modified algorithm in [8] to construct an admissible discrete vector field and also to check the cellularity condition in each step.

It should be mentioned that the class of finite topological spaces to which these results can be applied has been extended in [3] to *quasicellular* spaces. The idea is to replace the degree function by the definition of a morphism $\rho : X \longrightarrow \mathbb{N}_0$ satisfying some particular conditions, in such a way that Theorems 1 and 2 are still valid and our algorithms can also be applied.

References

[1] ALEXANDROFF P., Diskrete Räume. *Mat. Sb. (N.S.)* **2**, 501–518 (1937).

[2] BARMAK, J.A., Algebraic topology of finite topological spaces and applications. *Lecture Notes in Mathematics Vol. 2032* (2011).

[3] CIANCI N. AND OTTINA M., A new spectral sequence for homology of posets. *Topology and its Applications* **217**, 1–19 (2017).

[4] CUEVAS ROZO J.L., Funciones submodulares y matrices en el estudio de los espacios topológicos finitos. *Maestria Thesis*, Universidad Nacional de Colombia, Bogotá, Colombia (2016).

[5] DOUSSON X., RUBIO J., SERGERAERT F. AND SIRET Y., The Kenzo program, Institut Fourier. *http://www-fourier.ujf-grenoble.fr/∼sergerar/Kenzo/* (1999).

[6] MCCORD M.C., Singular homology groups and homotopy groups of finite topological spaces. *Duke Math. J.* **33**(3), 465–474 (1966).

[7] MINIAN E. G., Some remarks on Morse theory for posets, homological Morse theory and finite manifolds. *Topology and its Applications*, **159**(12), 2860–2869 (2012).

[8] ROMERO A. AND SERGERAERT F., Discrete Vector Fields and Fundamental Algebraic Topology. EPrint: *2010arXiv1005.5685R* (2010).

[9] STONG R.E., Finite topological spaces. *Trans. Amer. Math. Soc.* **123**(2), 325–340 (1966).

[1]Department of Mathematics
National University of Colombia
jlcuevasr@unal.edu.co
hsarriaz@unal.edu.co

[2]Department of Mathematics and Computer Science
University of La Rioja
ana.romero@unirioja.es
lalamban@unirioja.es

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Maximal Stable Homological Regions and AT-models*

H. Molina-Abril[1], **P. Real**[1], **F. Díaz-del-Río**[1]

Keywords: Maximal Stable Homological Regions, Homological Segmentation, AT-model

Let X be a finite cell complex. Working with $Z/2Z$ as the ground ring, we construct from an AT-model [1] a partition of X as a set of cells, called *a homological segmentation* of X. Its regions are strongly related to the specification of the homological holes of X as set of cells in which paths cutting or delineating them live. This method can be curiously seen as a purely homological version of the computer vision procedure named *maximally stable extremal regions (MSER)* proposed by Matas et al [2], which is used as a method of blob detection in digital images. In this sense, we show some experiments with three-dimensional digital objects in order to analyze the mathematical notion of homological segmentation within the context of topological object recognition.

References

[1] P. PILARCZYK, P. REAL, Computation of cubical homology, cohomology and (co)homological operations via chain contractions. *Adv. Comput. Math.*, **41**(1), 253-275 (2015).

[2] J. MATAS, O. CHUM, M. URBAN, T. PAJDLA, Robust wide baseline stereo from maximally stable extremal regions." In *Proc. of British Machine Vision Conference* 384-396 (2002).

[1]HTS. Informatics Engineering
University of Seville
Seville (Spain)
real@us.es

*This work has been supported by the Spanish research project TOP4COG (Topological Recognition of 4D Digital Images via HSF model, MTM2016-81030-P (AEI/FEDER,UE))

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Computing Homotopy Information of 4D Digital Objects in Parallel*

P. Real[1], **F. Díaz-del-Río**[1], **H. Molina-Abril**[1], **D. Onchis-Moaca**[2], **S. Blanco-Trejo**[1]

Keywords: four-dimensional digital object, primal-dual abstract cell complex, homology, homotopy,

Let $X \subset I$ be a digital object embedded in a 4-dimensional digital image I. Working with a primal-dual abstract cell complex (pACC, for short) version $pACC(X)$ of X , we design an algorithm in which elementary homotopy operations can be exhaustively applied to $pACC(X)$ in order to obtain a smaller pACC (in terms of cells and connexions between them) whose cells are strongly related to the integer algebraic homological generators of $pACC(X)$. An ambiance-based parallel version of this previous algorithm can be designed from which homology and homotopy Information of X can be derived in a straightforward manner.

References

[1] P. REAL, F. DÍAZ-DEL-RÍO, D. ONCHIS, Toward Parallel Computation of Dense Homotopy Skeletons for nD Digital Objects. International Workshop on Combinatorial Image Analysis. IWCIA 2017, 142-155 (2017).

[1]HTS. Informatics Engineering
University of Seville
Seville (Spain)
real@us.es

[2]Faculty of Mathematics, University of Vienna, Oskar-Morgenstern-Platz 1, A-1090 Wien, Austria and
Faculty of Mathematics and Computer Science, West Univ. of Timisoara, Vasile Parvan St. no. 4, Timisoara, Romania

*This work has been supported by the Spanish research project TOP4COG (Topological Recognition of 4D Digital Images via HSF model, MTM2016-81030-P (AEI/FEDER,UE))

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Reductions of monomial resolutions for the computation of high dimensional simplicial homology

E. Sáenz-de-Cabezón[1]

Abstract

In this paper we propose an algorithm for the computation of monomial resolutions that can be useful for obtaining the reduced homology of simplicial complexes. The algorithm is based on the reduction of known resolutions using the support of smaller ones. We start with a combinatorial resolution that is highly non minimal but easy to obtain, such as Taylor resolution. On the other hand, we compute in a combinatorial way the support of a smaller resolution (without computing the differentials in this resolution). In this step we use Mayer-Vietoris tree algorithm to obtain the support of a mapping cone resolution. Finally the last step consists on reducing the differential of the Taylor resolution using the information in the support of the mapping cone resolution to have smaller matrices, from which we compute the homology of the given simplicial complex.

Usually, a simplicial complex is given by a list of its facets. It is important to note that we use the ideal generated by the complements of the facets of the simplicial complex, which is equivalent to use the ideal generated by the minimal nonfaces, however, passing from one representation to the other is computationally demanding. Due to the size of the matrices involved in this process, our algorithm is particularly useful for simplicial complexes of high dimensions, since the matrices in the usual algorithm grow exponentially in terms of dimension of the complex, and those in our approach grow exponentially in terms of the number of facets of the complex.

References

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

[2] H. Charalambous and E. G. Evans, Resolutions obtained as iterated mapping cones, Journal of Algebra, 176, 1995, pp. 750–754

[3] J. G. Dumas, F. Heckenbach, D. Saunders and V. Welker, Computing simplicial homology based on efficient Smith normal form algorithms, in M. Joswig and N. Takayama (eds.) Algebra, Geometry and Software Systems, Springer, 2003.

[4] J. Herzog and Y. Takayama, Resolutions by mapping cones, Homology, homotopy and Applications 4(2) 2002, pp. 277-294

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

[6] 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

[7] D. Taylor, Ideals generated by monomials in an R-sequence, PhD Thesis, University of Chicago (1960)

[1]Universidad de La Rioja
eduardo.saenz-de-cabezon@unirioja.es

S5

Computer Algebra for Dynamical Systems and Celestial Mechanics

Celestial Mechanics and Dynamical Systems are traditional fields for applications of computer algebra. Computer algebra methods play a fundamental role in the treatment of concrete problems and applications. Computer algebra applications include nontrivial use of existing systems Maple, Mathematica, Singular etc. and the development and implementation of new algorithms, and specialized packages. The session will bring together specialists from diverse areas: differential equations, dynamical systems and computer algebra. Expected topics of presentations include (but are not limited to):

- Stability and bifurcation analysis of dynamical systems
- Construction and analysis of the structure of integral manifolds
- Symplectic methods
- Symbolic dynamics
- Celestial mechanics and stellar dynamics. N-body problem, KAM theory
- Specialized computer algebra software for celestial mechanics
- Normal form theory and formal integrals
- Deterministic chaos in dynamical systems
- Families of periodic solutions
- Perturbation theories and reductions
- Exact solutions and partial integrals
- Analysis and blow-ups of non-elementary stationary points
- Analysis of singularities: geometry and topology

- Integrability and nonintegrability, algebraic invariant sets and Darboux integrability
- Discrete Dynamical Systems and ergodic theory
- Topological structure of phase portraits and computer visualization

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

On the Numerical Analysis and Visualisation of Implicit Ordinary Differential Equations

Elishan Braun[1], **Werner M. Seiler**[2], **Matthias Seiß**[2]

We discuss how the geometric theory of differential equations [4] can be used for the numerical integration and visualisation of implicit ordinary differential equations, in particular around singularities of the equation [3]. The Vessiot theory [2] automatically transforms an implicit differential equation into a vector field distribution on a manifold and thus reduces its analysis to standard problems in dynamical systems theory like the integration of a vector field and the determination of invariant manifolds. For the visualisation of low-dimensional situations we adapt the streamlines algorithm of Jobard and Lefer to 2.5 and 3 dimensions. A concrete implementation in Matlab is presented [1].

Keywords: Implicit ordinary differential equations, Vessiot distribution, jet bundles, singular points, invariant manifolds

References

[1] E. BRAUN, *Numerische Analyse und Visualisierung von voll-impliziten gewöhnlichen Differentialgleichungen*. Master thesis, Institut für Mathematik, Universität Kassel (2017)

[2] D. FESSER; W.M. SEILER, Existence and Construction of Vessiot Connections. *SIGMA* **5**, 092 (2009)

[3] U. KANT; W.M. SEILER, Singularities in the Geometric Theory of Differential Equations. In *Dynamical Systems, Differential Equations and Applications 2*, W. Feng et al. (eds.) , 784–793, AIMS 2012

[4] W.M. SEILER, *Involution*. Springer-Verlag, Berlin, 2010.

[1]Departimento di Matematica e Fisica
Università degli Studi Roma Tre
Largo San Leonardo Murialdo 1, 00146 Rome, Italy
elishan@hotmail.de

[2]Institut für Mathematik
Universität Kassel
Heinrich-Plett-Straße 40, 34132 Kassel, Germany
[seiler,mseiss]@mathematik.uni-kassel.de

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Singular Initial Value Problems for Quasi-Linear Ordinary Differential Equations

Werner M. Seiler[1], **Matthias Seiß**[1]

We discuss existence, non-uniqueness and regularity of solutions of initial value problems for quasi-linear ordinary differential equations where the initial condition corresponds to an impasse point [4] of the equation. With a differential geometric approach [1, 3], we reduce the problem to questions in dynamical systems theory. As an application, we discuss in detail second-order equations of the form $g(x)u'' = f(x, u, u')$ with an initial condition imposed at a simple zero of g. This generalises results by Liang [2] and also makes them more transparent via our geometric approach.

Keywords: Quasi-linear ordinary differential equations, geometric theory, initial value problem, existence and (non-)uniqueness of solutions, regularity

References

[1] D. FESSER; W.M. SEILER, Existence and Construction of Vessiot Connections. *SIGMA* **5**, 092 (2009)

[2] J.F. LIANG, A singular initial value problem and self-similar solutions of a nonlinear dissipative wave equation. *J. Diff. Eqs.* **246**, 819–844 (2009)

[3] W.M. SEILER, *Involution*. Springer-Verlag, Berlin, 2010.

[4] W.M. SEILER, Singularities of implicit differential equations and static bifurcations. In *Computer Algebra in Scientific Computing – CASC 2013*, V. Gerdt et al. (eds.), 355–368, Springer-Verlag, Chaim, 2013

[1]Institut für Mathematik
Universität Kassel
Heinrich-Plett-Straße 40, 34132 Kassel, Germany
[seiler,mseiss]@mathematik.uni-kassel.de

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

The construction of averaged semi-analytical planetary motion theory up to the third degree of planetary masses by means CAS Piranha

Alexander Perminov[1], **Eduard Kuznetsov**[1]

The study of planetary systems orbital evolution is one of important problems of Celestial mechanics. In this work authors present the algorithm for the construction of the averaged semi-analytical motion theory up to the third degree of the small parameter for the case of planetary system with four planets. In this case the small parameter is the ratio of sum of planetary masses to the mass of the star.

The Hamiltonian of four-planetary problem is written in Jacobi coordinates and it is expressed into the Poisson series in elements of Poincare's second system. It allows sufficiently simplifying an angular part of the series expansion. In this case only one angular element – mean longitude, is defined.

The averaged Hamiltonian and the motion equations in averaging elements are constructed by Hori-Deprit method as the series in the small parameter and all orbital elements. The transformation between osculating and averaged orbital elements is performed by using of the functions for the change of variables. The using of the averaged motion equations allows sufficiently increase time step of the next numerical integration.

All analytical manipulations are performed by using of computer algebra system Piranha [1]. The author of Piranha system is Francesco Biscani from Max Plank Institute for Astronomy in Heidelberg, Germany. Piranha is echeloned Poisson series processor. It is developing C++ code with Python interface for analytical calculations with polynomials, Poisson series and echeloned Poisson series.

Orbital elements and masses are kept in the series expansions as symbol variables. It should be noted that series numerical coefficients are kept as rational numbers with arbitrary precision for the elimination of rounding errors.

The terms with the first order of the small parameter in the averaged Hamiltonian is constructed up to 8-th degree of eccentric and oblique Poincare elements. The second order terms is constructed up to 6-th degree and the third order terms – up to 2-nd degree of eccentric and oblique Poincare elements. It allows to get high precision motion equations for giant planets of Solar system and various extrasolar systems also. The algorithms of the expansion into the Poisson series and the construction of motion equations are presented in this work.

The results of numerical integration of the motion equations for the Sun – Jupiter – Saturn – Uranus – Neptune's system on a time interval of 10 billion years is considered. It is performed by Everhart method of 15-th order. The motion of the planets

has an almost periodic character. The orbital eccentricities and inclinations save small values over whole time of the integration. The comparison with numerical theories is given.

The study was funded by RFBR according to the research project no. 18-32-00283 and the Government of the Russian Federation (Act no. 211, agreement no. 02.A03.21.0006).

Keywords: CAS Piranha, echeloned Poisson series processor, four-planetary problem, semi-analytical motion theory, Hori-Deprit method, Jacobi coordinates, second system of Poincare elements

References

[1] F. BISCANI, *The Piranha computer algebra system*. https://github.com/bluescarni/piranha, 2018

[1]Chair of astronomy, geodesy and environmental monitoring
Ural Federal University
620000, 51 Lenin Avenue, Ekaterinburg, Russia
perminov12@yandex.ru

[1]Chair of astronomy, geodesy and environmental monitoring
Ural Federal University
620000, 51 Lenin Avenue, Ekaterinburg, Russia
eduard.kuznetsov@urfu.ru

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Local and Global Properties of ODEs*

Victor Edneral[1], **Valery Romanovski**[2]

We consider autonomous planar systems of ordinary differential equations with a polynomial nonlinearity. These systems are resolved with respect to derivatives and can contain free parameters. To study local integrability of the system near each stationary points, we use an approach based on Power Geometry[1] and on the computation of the resonant normal form[2, 3]. For the pair of concrete planar systems[4] and[5], we found the complete set of necessary conditions on parameters of the system for which the system is locally integrable near each stationary points. The main idea of this report is in the hypothesis that if for each fixed set of parameters such that all stationary points of the equation are centers then this system has the global first integral of motion. So from some finite set of local properties we can obtain a global property. But if the system has some invariant lines or separatists, this first integral can exist only in the part of the phase space, where center points take place.

Keywords: Local Integrability, Global Integrability

References

[1] A.D. Bruno. *Power Geometry in Algebraic and Differential Equations*, Fizmatlit, Moscow, 1998 (Russian) = Elsevier Science, Amsterdam, 2000 (English).

[2] A.D. Bruno, *Local Methods in Nonlinear Differential Equations*, Nauka, Moscow, 1979 (Russian) = Springer-Verlag, Berlin, 1989 (English).

[3] V.F. Edneral, *On algorithm of the normal form building*, in: Ganzha et al. (Eds.) Proceedings of the CASC 2007, Springer-Verlag series: LNCS 4770 (2007) 134–142.

[4] A. Algaba, E. Gamero, C. Garcia, The integrability problem for a class of planar systems, Nonlinearity v. 22 (2009) 395–420

[5] V.A. Lunkevich, K.S. Sibirskii, *Integrals of General Differential System at the Case of Center. Differential Equation*, v. 18, No 5 (1982) 786–792 (Russian).

*The publication has been prepared with the support of the "RUDN University Program 5-100" and funded by RFBR according to the research projects No. 12-34-56789 and No. 12-34-56789. Valery Romanovski acknowledges the financial support from the Slovenian Research Agency (research core funding No. P1-0306 and project N1-0063).

[1]Peoples' Friendship University of Russia (RUDN University)
6 Miklukho-Maklaya st., Moscow, 117198, Russian Federation

Skobeltsyn Institute of Nuclear Physics
Lomonosov Moscow State University
Leninskie Gory 1(2), Moscow, 119991, Russian Federation
edneral_vf@pfur.ru

[2]Faculty of Electrical Engineering and Computer Science
University of Maribor
Koroška cesta 46, Maribor, SI-2000 Maribor,

CAMTP – Center for Applied Mathematics and Theoretical Physics
University of Maribor
Mladinska 3, Maribor SI-2000

Faculty of Natural Science and Mathematics
University of Maribor
Koroška cesta 160, SI-2000 Maribor, Slovenia
valery.romanovsky@uni-mb.si

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Nonlinear Oscillations of a Spring Pendulum at the 1 : 1 : 2 Resonance by Normal Form Method*

Victor Edneral[1], **Alexander Petrov**[2]

Nonlinear spatial oscillations of a material point on a weightless elastic suspension are considered. The frequency of vertical oscillations is assumed to be equal to the doubled swinging frequency (the 1 : 1 : 2 resonance) [1]. In this case, vertical oscillations are unstable, which leads to the transfer of the energy of vertical oscillations to the swinging energy of the pendulum. Vertical oscillations of the material point cease, and, after a certain period of time, the pendulum starts swinging in a vertical plane. This swinging is also unstable, which leads to the back transfer of energy to the vertical oscillation mode, and again vertical oscillations occur. However, after the second transfer of the energy of vertical oscillations to the pendulum swinging energy, the apparent plane of swinging is rotated through a certain angle. These phenomena are described analytically by the normal form method[2].

Keywords: Pendulum, Resonance, Normal form method

References

[1] A. G. Petrova,b and V. V. Vanovskiya, *Nonlinear Oscillations of a Spring Pendulum at the 1 : 1 : 2 Resonance: Theory, Experiment, and Physical Analogies*, Nauka, Moscow, Trudy Matematicheskogo Instituta imeni V.A. Steklova, 2018, Vol. 300, pp. 168–175.

[2] V.F. Edneral, *On algorithm of the normal form building*, in: Ganzha et al. (Eds.) Proceedings of the CASC 2007, Springer-Verlag series: LNCS 4770 (2007) 134–142.

[1]Peoples' Friendship University of Russia (RUDN University)
6 Miklukho-Maklaya st., Moscow, 117198, Russian Federation

Skobeltsyn Institute of Nuclear Physics
Lomonosov Moscow State University
Leninskie Gory 1(2), Moscow, 119991, Russian Federation
edneral_vf@pfur.ru

*The publication has been prepared with the support of the "RUDN University Program 5-100" and funded by RFBR according to the research projects No. 12-34-56789 and No. 12-34-56789).

[2]Ishlinsky Institute for Problems in Mechanics of the Russian Academy of Sciences
Prosp. Vernadskogo 101(1), Moscow, 119526, Russian Federation
petrovipmech@gmail.com

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

On the estimation of complexity of trajectories in the equal-mass free-fall three-body problem

Mylläri Aleksandr[1], **Mylläri Tatiana**[1], **Myullyari Anna**[2], **Vassiliev Nikolay**[3]

We study complexity of trajectories in the equal mass free-fall three-body problem. We construct numerically symbolic sequences using different methods: close binary approaches, triple approaches, collinear configu- rations and other. Different entropy estimates for individual trajectories and for a system as a whole are compared.

Keywords: Three-Body Problem, Symbolic Dynamics, Entropy

[1]Dept. of Computers & Technology, SAS
St.George's University
St.George's, Grenada, West Indies
amyllari@sgu.edu

[2]Accendo Data LLC
Coral Springs,
Florida, USA
anna.myullyari@accendodata.com

[3]V.A. Steklov Institute of Mathematics
of the Russian Academy of Sciences
St. Petersburg, Russia
vasiliev@pdmi.ras.ru

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Schutzenberger transformation on the three-dimensional Young graph

Vasilii Duzhin[1], **Nikolay Vassiliev**[1,2]

The Schutzenberger transformation on Young tableaux, also known as "jeu de taquin", was introduced in [1]. This transformation allows to solve different problems of enumerative combinatorics and representation theory of symmetric groups. Particularly, it can be used to calculate the Littlewood-Richardson coefficients [2].

It is known [3] that a limit distribution of Plancherel probabilities on the front of large Young diagrams of size $n, n \to \infty$ has the following density function known as semicircle distribution:

$$d\mu(u) = \frac{\sqrt{4-u^2}}{2 \cdot \pi},$$

where u is one of Vershik-Kerov coordinates: $u = \frac{x-y}{\sqrt{n}}$. Later it was proved [4] that the coordinates of Schutzenberger path ends are distributed according to the semicircle distribution as well.

However, there are no known limit distribution function of the coordinates of three-dimensional Schutzenberger path ends. Moreover, there are no known 3D analogues of the central Plancherel process and RSK correspondence. In this work we made an attempt to fill this gap by conducting some numerical experiments on the three-dimensional Young graph.

Also we considered a special randomized variant of the Schutzenberger transformation. It was found that this approach can be used to calculate the co-transition probabilities on the Young graph, which in turn gives a possibility to calculate the ratios of dimensions of 3D Young diagrams. Note that the exact dimensions of 3D Young diagrams cannot be calculated directly.

Keywords: Young tableaux, Young diagrams, Schutzenberger transformation, Jeu de taquin, Limit shape

References

[1] M. P. SCHÜTZENBERGER, "Quelques remarques sur une construction de Schensted", *Math. Scandinavica* 12, (1963), 117-128.

[2] S. V. Fomin, Knuth equivalence, jeu de taquin, and the Littlewood-Richardson rule, Appendix 1 to Chapter 7 in: R.P.Stanley, Enumerative Combinatorics, vol 2, Cambridge University Press.

[3] S. V. Kerov, "Transition Probabilities for Continual Young Diagrams and the Markov Moment Problem", *Funktsional. Anal. i Prilozhen.*, 27:2 (1993), 32–49; *Funct. Anal. Appl.*, 27:2 (1993), 104–117

[4] Dan Romik and Piotr Sniady. Jeu de taquin dynamics on infinite Young tableaux and second class particles. *Annals of Probability: An Official Journal of the Institute of Mathematical Statistics*, 43(2):682-737, 2015

[1]Faculty of Computer Science and Technology
Saint Petersburg Electrotechnical University
ul. Professora Popova 5, 197376 St. Petersburg, Russia
vduzhin.science@gmail.com

[2]Laboratory of Representation Theory and Dynamical Systems
St.Petersburg department of Steklov Institute of mathematics RAS
27, Fontanka, 191023 St.Petersburg, Russia
vasiliev@pdmi.ras.ru

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

The modeling of the effect of velocity of breakup in osculating orbital elements of the young asteroid family

Rosaev A.[1]

Asteroid families are groups of minor planets that have a common origin in breakup events. The very young compact asteroid clusters (VYF) with age smaller than 1 Myr allow us to study impact process and nonlinear dynamics. In previous our paper [1] we had noted dependence between $d\Omega$ and $d\varpi$ for Datura family but had not explained it. Additionally, we find other dependences between angular elements $d\omega$ and $d\varpi$ in some other very young asteroid family. Vokrouhlicky et al. [2] have given explanation but their model cannot proper explain value of observed slope. In this paper we test the hypothesis of the primordial origin of the observed dependences at the epoch of the cluster formation. The implicit dependences of the orbital elements on breakup velocity components are studied with Maple. As a result, the dependences, similar to observed, obtained at specific values of breakup velocities.

Keywords: asteroid family, orbital evolution, breakup velocity

References

[1] A. ROSAEV; E. PLAVALOVA,New members of Datura family, *Planetary and Space Science*, **140**, 21-26 (2017).

[2] D. VOKROUHLICKY, ET AL, The young Datura asteroid family. Spins, shapes, and population estimate. *Astronomy and Astrophysics*, **598**, A91 (2017).

[1]Research and Educational Center "Nonlinear Dynamics",
Yaroslavl State University

hegem@mail.ru

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Searching for periodic solutions with central symmetry in Hill problem*

Alexander Batkhin[1],

We consider Hill problem (see [1, 2]) describing the motion of massless body near the minor of two active masses as a regular perturbation of Kepler problem in uniformly rotating (sinodical) frame. It makes possible to apply the classical method of Hamiltonian normal form [3] for searching generating solutions of families of periodic orbits. The essential difference of the Hill problem from the well-known Restricted Three Body Problem (RTBP) is that canonical equations of motions are invariant under the group of linear transformations of the extended phase space with generators:

$$\Sigma_1 : (t, x_1, x_2, y_1, y_2) \to (-t, x_1, -x_2, -y_1, y_2)\,,$$
$$\Sigma_2 : (t, x_1, x_2, y_1, y_2) \to (-t, -x_1, x_2, y_1, -y_2)\,,$$

This fact allows two state that the set of periodic solutions can be divided into following subsets:

- asymmetric orbits, which change under any transformation;
- singly symmetric orbits, which are invariant under transformation Σ_1 or Σ_2;
- centrally symmetric orbits, which are invariant under composition $\Sigma_{12} \equiv \Sigma_1 \circ \Sigma_2$ only;
- doubly symmetric orbits, which are invariant under any transformation.

Earlier [2, 4], periodic solutions with any type of symmetry but central were computed. This work is an attempt to find generating solutions with central symmetry and to continue them into periodic solutions of the Hill problem.

Just now the following steps are realized:

1. generalized Hill problem Hamiltonian with small parameter ε is rewritten in Delaunay variables;
2. the procedure of invariant Hamiltonian normalization up to the second order is applied;

*RFBR project No. 18-01-00422

3. the condition on existing of generating solutions can be written in the form

$$F(e,p,q)\sin k\varpi = 0,$$

where e is an eccentricity, ϖ is an argument of the pericenter, $p+q \in \{1,2,4\}$. Function $F(e,p,q)$ is smooth for $e \in [0;1)$. The parameter k equals to 2 for $p+q=1$ or 2, equals to 4 for $p+q=4$.

The specific of the generalized Hill problem leads to the evidence that it is possible to successfully continue such generating solutions into the Hill problem periodic orbits, which major semi-axis a is less then 1, or $p,q \in \mathbb{N}$. For centrally symmetric generating solutions it is possible if $p > 2$, p is odd, and $\varpi \neq k\pi/4$, $k \in \mathbb{N}$. A suitable for continuation generating solution corresponds to the only values $p = 3$ and $e \approx 0.8525432355$.

Keywords: Hill problem, periodic solution, symmetry

References

[1] V. SZEBEHELY, *Theory of Orbits. The Restricted Problem of Three Bodies*. Academic Press, New York and London, 1967.

[2] A. B. BATKHIN; N. V. BATKHINA, *Hill Problem*. Volgogradskoe nauchnoe izdatel'stvo, Volgograd, 2009 (in Russian).

[3] A. D. BRUNO, *The Restricted 3–body Problem: Plane Periodic Orbits*. Walter de Gruyter, Berlin, 1994.

[4] A. B. BATKHIN, New families of doubly symmetric periodic solutions of Hill problem. *IEEE RUSSIA, MOSCOW*, **1**, 1–4, 2016.

[1]Singular Problem Department
Keldysh Institute of Applied Mathematics of RAS
Miusskaya sq. 4, Moscow, 125047, Russia
batkhin@gmail.com

S6

Computational Differential and Difference Algebra

Algebraic differential and difference equations and systems of such equations arise in many areas of mathematics, natural sciences and engineering. One can say that difference equations relate to differential equations as discrete mathematics relates to continuous mathematics. Differential / difference computer algebra studies algebraic differential / difference equations in a constructive way that extends the methods and algorithms of commutative algebra and algebraic geometry. The main goal of the session is to consider the computational problems in differential/difference algebra to explore new constructive ideas and approaches oriented toward various applications.

Expected topics of presentations include (but are not limited to):

- Differential and Difference Equations and Systems
- Differential and Difference Gröbner (Standard) and Involutive Bases
- Differential and Difference Characteristic Sets
- Triangular Decompositions of Differential and Difference Systems
- Differential and Difference Elimination
- Algorithmic Generation of Finite Difference Approximations to PDEs
- Consistency and Stability Analysis of Finite Difference Approximations
- Difference-Differential Polynomials and Systems
- Software Packages for Differential and Difference Algebra
- Applications of Differential and Difference Algebra in Mathematics and Natural Sciences

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Bounds for Proto-Galois Groups

Eli Amzallag[1], **Andrei Minchenko**[2], **Gleb Pogudin**[3]

In studying linear differential equations of the type $Y' = AY, A \in M_n(C(t))$, it is often important to investigate the algebraic or differential relations among the solutions. The benefit of obtaining such data is that it can be used to anticipate the computational power needed to express solutions. In [4], Kolchin made this precise by establishing a link between how solutions to $Y' = AY$ might be expressed and different properties of the corresponding differential Galois group, an object he constructed exactly to capture relations among the solutions. These differential Galois groups can be realized as linear algebraic groups. In fact, many algorithms to compute them have been developed since Kolchin's foundational discussions of these results in [4] and [5].

Kovacic [6] proposed an algorithm for second-order differential equations. Compoint and Singer also provided an algorithm in [1] that can be applied to equations of any order, if it is known in advance that the differential Galois group is reductive. A general algorithm for computing the differential Galois group was designed by Hrushovski [3]. Making this algorithm practical and understanding its complexity is an important challenge. Hrushovski conjectured that none of its steps would "require more than doubly exponential time." In [2], Feng expounded on the details of Hrushovski's original algorithm with differential-algebraic terminology and improved the algorithm. He also formally defined an object computed in the first step of the algorithm, a proto-Galois group. Such a group is an algebraic group, contains the differential Galois group, and the computation of it allows one to reduce the computation of the differential Galois group to the hyperexponential case, which is addressed by the algorithm in [1]. In Hrushovski's algorithm, a proto-Galois group is computed by making an ansatz based on an a priori bound for the degrees of defining polynomials of the group. Thus, such a bound is an essential part of the algorithm. Moreover, it also needed for understanding the complexity of the algorithm.

In [2], Feng showed that there exists a proto-Galois group defined by polynomials of degree at most sextuply exponential in n. Sun [7] utilized triangular sets in place of the Groebner bases used by Feng. This different choice of representation for a group leads to a bound triply exponential in n.

We adopt a different emphasis from both Feng and Sun. Instead of focusing on equations for the group's corresponding radical ideal, we take a more geometric approach and focus on equations that define a proto-Galois group as an algebraic variety in $GL_n(C)$. In conjunction with exploiting the structural theory of algebraic groups, this approach allows us to further improve on Feng's bound and thereby improve the algorithm. We obtain an explicit bound of the form $n^{O(n^4)}$.

We also assess the practicality of using Hrushovski's algorithm for $n = 2, 3$, the cases that arise most often in applications. We expect to determine tighter bounds than our general bound suggests for these cases. In fact, we have established a tighter bound for $n = 2$, for which our final bound is 6. We will discuss how we obtained this result. We will also discuss work in progress for $n = 3$ and extending our methods for $n = 2$ to those cases.

Keywords: Algebraic Geometry, Group Theory and Generalizations, Ordinary Differential Equations

References

[1] E. COMPOINT; M.F. SINGER, Computing Galois groups of completely reducible differential. *Journal of Symbolic Computation*, **28**(4-5), 473–494 (1999).

[2] R. FENG, Hrushovski's algorithm for computing the Galois group of a linear differential equation. *Advances in Applied Mathematics*, **65**, 1–37 (2015).

[3] E. HRUSHOVSKI, Computing the Galois group of a linear differential equation. *Banach Center Publications*, **58**(1), 97–138 (2002).

[4] E. R. KOLCHIN, The Picard-Vessiot Theory of Homogeneous Linear Ordinary Differential Equations. *Proceedings of the National Academy of Sciences*, **32**(12), 308-311 (1946).

[5] E. R. KOLCHIN, Algebraic Matric Groups. *Proceedings of the National Academy of Sciences*, **32**(12), 306-308 (1946).

[6] J. J. KOVACIC, An algorithm for solving second order linear homogeneous differential equations. *Journal of Symbolic Computation*, **2**(1), 3–43 (1986).

[7] M. SUN, A New Bound on Hrushovski's Algorithm for Computing the Galois Group of a Linear Differential Equation. *Preprint*, 2018. URL https://arxiv.org/abs/1803.07105

[8] J. VAN DER HOEVEN, Around the numeric–symbolic computation of differential Galois groups. *Journal of Symbolic Computation*, **42**(1-2), 236–264 (2007).

[1]Department of Mathematics
CUNY Graduate Center
365 5th Avenue
New York, NY 10016
eamzallag@gradcenter.cuny.edu

[2]Department of Statistical and Actuarial Sciences
University of Western Ontario
Western Science Centre - Room 262 - 1151 Richmond Street
London, Ontario, Canada, N6A 5B7
aminche@uwo.ca

[3]Courant Institute of Mathematical Sciences
New York University
251 Mercer Street
New York, NY 10012
pogudin@cims.nyu.edu

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

The global dimension of the algebras of integro-differential operators and their factor algebras

V. V. Bavula[1]

We discuss some homological properties of the algebras of integro-differential operators and their factor algebras. In particular, their global dimension and weak homological dimensions are found.

Keywords: the algebra of integro-differential operators, the weak homological dimension, the global dimension

[1]School of Mathematics and Statistics
University of Sheffield
Hounsfield Road, UK
v.bavula@sheffield.ac.uk

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Effective calculation in studying the Jacobian Conjecture

Paweł Bogdan[1]

In 1930s Keller stated a problem which is known nowadays as the Jacobian Conjecture. In [1] Crespo and Hajto gave an equivalent condition to this Conjecture in a language of Picard-Vessiot theory. They also gave an effective criterion to determine whether a given polynomial map is an automorphism. Their result was improved in [2].

The work on this improvement led me to propose a method to invert polynomial maps $F = (F_1, ..., F_n)$ on a field K such that, for every $i \in \{1, ..., n\}$ $F_i = X_i + H_i$, where H_i has a vanishing order at least 2. My algorithm does not perform derivatives neither division so it can be applied to maps over finite fields. A description of the algorithm can be found in [3] and an estimation of its computational complexity can be found in [4].

In my talk I will present the algorithm and the estimation of its complexity. I will also discuss effective implementations of it on various Computer Algebra Systems.

Keywords: polynomial automorphisms, Jacobian Conjecture, algorithmics

References

[1] T. CRESPO, Z. HAJTO, Picard-Vessiot theory and the Jacobian problem. *Israel Journal of Mathematics* **186**, 243-248 (2011).

[2] E. ADAMUS, P. BOGDAN, Z. HAJTO, An effective approach to Picard-Vessiot theory and the Jacobian Conjecture. *Schedae Informaticae* **26** (2017).

[3] E. ADAMUS, P. BOGDAN, T. CRESPO, Z. HAJTO, An effective study of polynomial maps. *Journal of Algebra and its applications* **16**(8) 13 pages (2017).

[4] P. BOGDAN, Complexity of the Inversion Algorithm of Polynomial Mappings . *Schedae Informaticae* **25** (2016).

[1]Chair of Effective Methods in Algebra
Faculty of Mathematics and Computer Science
Jagiellonian University
ul. Łojasiewicza 6, 30-348 Kraków, Poland
bogdan@ii.uj.edu.pl

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Formal Power Series Solutions of First Order Autonomous Algebraic Ordinary Differential Equations*

Sebastian Falkensteiner[1], **J.Rafael Sendra**[2]

Let $\mathbb{K}$ be an algebraically closed field of characteristic zero. Given a first order autonomous algebraic ordinary differential equation, i.e. an equation of the form

$$F(y, y') = 0 \text{ with } F \in \mathbb{K}[y, y'],$$

we present a method to compute all formal power series solutions. Furthermore, by choosing for instance $\mathbb{K} = \mathbb{C}$, the computed formal power series solutions are indeed convergent in suitable neighborhoods.

We follow the algebro-geometric approach by Feng and Gao [2] and consider y and y' as independent variables, let us say y and z. Then F implicitly defines an affine plane curve where local parametrizations can be computed, see e.g. [3]).

We show a sufficient and necessary condition on such a local parametrization to obtain a formal power series solution of the original differential equation by substitution. Moreover, we present a polynomial-time algorithm for computing all the initial tuples, i.e. the first two coefficients of a formal power series, which can be extended to a solution. By choosing a particular initial tuple, a second algorithm determines the coefficients of all solutions starting with this initial tuple up to an arbitrary order.

A full version [1] has been submitted to a journal and is online available.

Keywords: Algebraic autonomous differential equation, algebraic curve, local parametrization, formal power series solution

References

[1] S. FALKENSTEINER AND J.R. SENDRA, *Formal Power Series Solutions of First Order Autonomous Algebraic Ordinary Differential Equations*. published in arXiv: 1803.04731, 2018.

*Authors supported by the Spanish Ministerio de Economía y Competitividad, by the European Regional Development Fund (ERDF), under the project MTM2017-88796-P. The first author also supported by the strategic program "Innovatives OÖ 2020" by the Upper Austrian Government and by the Austrian Science Fund (FWF): P 31327-N32.

[2] R. FENG AND X.-S. GAO, *Rational general solutions of algebraic ordinary differential equations*. In *Proceedings of the 2004 international symposium on Symbolic and algebraic computation*, pages 155–162. ACM, New York, 2004.

[3] R.J. WALKER, *Algebraic curves*. Princeton University Press, Princeton, 1950.

[1]Research Institute for Symbolic Computation (RISC)
Johannes Kepler University Linz
Altenbergerstraße 69, 4040 Linz, Austria
falkensteiner@risc.jku.at

[2]Research Group ASYNACS. Dpto. de Física y Matemáticas
Universidad de Alcalá
E28871 Alcalá de Henares, Madrid, Spain
Rafael.sendra@uah.es

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Dimension Polynomials and the Einstein's Strength of Some Systems of Quasi-linear Algebraic Difference Equations

Alexander Evgrafov[1], **Alexander Levin**[2]

We present a difference algebraic technique for the evaluation of the Einstein's strength of quasi-linear partial difference equations and some systems of such equations. Our approach is based on the properties of difference dimension polynomials that express the Einstein's strength and on the characteristic set method for computing such polynomials. The obtained results are applied to the comparative analysis of difference schemes for some chemical reaction-diffusion equations.

Keywords: Difference dimension polynomial, Autoreduced set, Einstein's strength

1 Preliminaries

Let K be an inversive difference field with a basic set of automorphisms $\sigma = \{\alpha_1, \ldots, \alpha_m\}$ and Γ the free commutative group generated by σ. If $\gamma = \alpha_1^{k_1} \ldots \alpha_m^{k_m} \in \Gamma$, then the number $\operatorname{ord} \gamma = \sum_{i=1}^{m} |k_i|$ is called the *order* of γ; if $r \in \mathbb{N}$, we set $\Gamma(r) = \{\gamma \in \Gamma \mid \operatorname{ord} \gamma \leq r\}$. In what follows we denote the set $\{\alpha_1, \ldots, \alpha_m, \alpha_1^{-1}, \ldots, \alpha_m^{-1}\}$ by σ^* and use the prefix σ^*- instead of "inversive difference". A reflexive difference ideal will be refer to as a σ^*-ideal.

Let $R = K\{y_1, \ldots, y_n\}^*$ be the ring of σ^*-polynomials in n σ^*-indeterminates over K. (As a ring, $R = K[\{\gamma y_i \mid \gamma \in \Gamma,\, 1 \leq i \leq n\}]$) An n-tuple $\xi = (\xi_1, \ldots, \xi_n)$ with coordinates in some σ^*-overfield K' of K is said to be a solution of the set of σ^*-polynomials $F = \{f_j \mid j \in J\} \subseteq R$ or a solution of the system of algebraic difference equations

$$f_j(y_1, \ldots, y_n) = 0 \ \ (j \in J) \tag{1}$$

if F is contained in the kernel of the natural difference K-homomorphism ("substitution") $R \to K'$ $(y_i \mapsto \xi_i)$. The system (1) is called *prime* if the σ^*-ideal P generated by the set F in R (it is denoted by $[F]^*$) is prime. In this case the quotient field L of R/P has a natural structure of a finitely generated σ^*-field extension of K: $L = K\langle \eta_1, \ldots, \eta_n \rangle^*$ where η_i is the canonical image of y_i in L. (As a field, $L = K(\{\gamma(\eta_i) \mid \gamma \in \Gamma,\, 1 \leq i \leq n\})$.) As it is proven in [3, Section 6.4], there exists a polynomial $\phi_{\eta|K}(t) \in \mathbb{Q}[t]$ such that

$\phi_{\eta|K}(r) = \operatorname{tr.deg}_K K(\{\gamma\eta_j | \gamma \in \Gamma(r), 1 \leq j \leq n\})$ for all sufficiently large $r \in \mathbb{Z}$.

This polynomial is called the σ^*-*dimension polynomial* of the σ^*-field extension L/K associated with the system of σ^*-generators $\eta = \{\eta_1, \ldots, \eta_n\}$. It is also said to be the σ^*-dimension polynomial of system (1). We refer to [3, Chapter 6] and [4, Chapters 4 and 7] for properties, invariants, and methods of computation of σ^*-dimension polynomials.

Let us consider a system of equations in finite differences with respect to unknown functions of m real (or complex) variables $x_1, \ldots, x_m$ that induces a prime system of algebraic difference equations. (The m basic automorphisms are defined by the shifts of the arguments: for any function $g(x_1, \ldots, x_m)$, $\alpha_i : g(x_1, \ldots, x_m) \mapsto g(x_1, \ldots, x_{i-1}, x_i + h_i, x_{i+1}, \ldots, x_m)$ where $h_1, \ldots, h_m$ are some real (or complex) numbers.) It is shown in [4, Section 7.7] that the σ^*-dimension polynomial of such a system expresses its strength in the sense of A. Einstein. This important characteristic of the system is a difference counterpart the concept of strength of a system of PDEs introduced in [1], see [4, Section 7.7] for details.

2 Autoreduced sets of quasi-linear σ^*-polynomials. Computation of the Einstein's Strength

With the above notation, let $\Gamma Y = \{\gamma y_i | \gamma \in \Gamma, 1 \leq i \leq n\} \subseteq R$; the elements of this set are called *terms*. The order $\operatorname{ord} u$ of a term $u = \gamma y_j$ is defined as the order of γ.

In what follows we consider the set $\mathbb{Z}^m$ as the union of 2^m *orthants* $\mathbb{Z}_j^{(m)}$ ($1 \leq j \leq 2^m$), that is, Cartesian products of m factors each of which is either $\mathbb{N} = \{k \in \mathbb{Z},\, k \geq 0\}$ or $\bar{\mathbb{Z}}_- = \{k \in \mathbb{Z},\, k \leq 0\}$. We set $\Gamma_j = \{\alpha_1^{k_1} \ldots \alpha_m^{k_m} \in \Gamma \,|\, (k_1, \ldots, k_m) \in \mathbb{Z}_j^{(m)}\}$ and $(\Gamma Y)_j = \{\gamma y_i \,|\, \gamma \in \Gamma_j, 1 \leq i \leq n\}$, so that $\Gamma Y = \bigcup_{j=1}^{2^m} (\Gamma Y)_j$. A term $v \in \Gamma Y$ is called a *transform* of a term $u \in \Gamma Y$ if u and v belong to the same set $(\Gamma Y)_j$ and $v = \gamma u$ for some $\gamma \in \Gamma_j$. We also fix an *orderly ranking* on ΓY, that is, a well-ordering $\leq$ of ΓY such that
(i) If $u \in (\Gamma Y)_j$ and $\gamma \in \Gamma_j$, then $u \leq \gamma u$; (ii) If $u, v \in (\Gamma Y)_j$, $u \leq v$ and $\gamma \in \Gamma_j$, then $\gamma u \leq \gamma v$; (iii) If $u, v \in \Gamma Y$ and $\operatorname{ord} u < \operatorname{ord} v$, then $u < v$.

If $A \in R$, then the greatest (with respect to $\leq$) term in A is called the *leader* of A; it is denoted by u_A. If $d = \deg_{u_A} A$ and A is written as a polynomial in u_A, then the coefficient of u_A^d is called the *initial* of A and is denoted by I_A. If $d = 1$ then the σ^*-polynomial A is called *quasi-linear*.

Let $A, B \in R$. The σ^*-polynomial A is said to be *reduced* with respect to B if A does not contain any power of a transform γu_B whose exponent is greater than or equal to $\deg_{u_B} B$. If $\mathcal{A} \subseteq R \setminus K$, then a σ^*-polynomial $A \in R$, is said to be reduced with respect to $\mathcal{A}$ if A is reduced with respect to every element of $\mathcal{A}$. A set $\mathcal{A} \subseteq R$ is said to be *autoreduced* if either $\mathcal{A} = \emptyset$ or $\mathcal{A} \bigcap K = \emptyset$ and the elements of $\mathcal{A}$ are reduced with respect to each other. As it is shown in [3, Section 3.4], distinct elements of an autoreduced set $\mathcal{A}$ have distinct leaders and every autoreduced set is

finite. Furthermore, if $A \in R$, then there exists a σ^*-polynomial $B \in R$ such that B is reduced with respect to $\mathcal{A}$ and $IB \equiv A(mod[\mathcal{A}]^*)$ where I is a product of transforms of initials of elements of $\mathcal{A}$. (We say that A *reduces to* B *modulo* $\mathcal{A}$.)

Let $A, B \in R$. We say that A has higher rank than B and write $\operatorname{rk} A > \operatorname{rk} B$ if either $A \notin K$, $B \in K$, or $u_B < u_A$, or $u_A = u_B$ and $\deg_{u_A} B < \deg_{u_A} A$. If $u_A = u_B$ and $\deg_{u_A} A = \deg_{u_A} B$, we say that A and B have the same rank and write $\operatorname{rk} A = \operatorname{rk} B$. Assuming that elements of an autoreduced set in R are arranged in the order of increasing rank, we compare such sets as follows: if $\mathcal{A} = \{A_1, \ldots, A_p\}$ and $\mathcal{B} = \{B_1, \ldots, B_q\}$, then $\mathcal{A}$ is said to have lower rank than $\mathcal{B}$ if either there exists $k \in \mathbb{N}$, $1 \leq k \leq \min\{p, q\}$, such that $\operatorname{rk} A_i = \operatorname{rk} B_i$ for $i < k$ and $\operatorname{rk} A_k < \operatorname{rk} B_k$, or $p > q$ and $\operatorname{rk} A_i = \operatorname{rk} B_i$ for $i = 1, \ldots, q$.

By [3, Proposition 3.4.30], every nonempty family of autoreduced sets contains an autoreduced set of lowest rank. If P is an ideal of R, then an autoreduced subset of P of lowest rank is called a *characteristic set* of P. Basic properties of characteristic sets are described in [4, Section 2.4]. In particular, it is shown that if P is generated by the σ^*-polynomials in the left-hand sides of a prime system of difference equations (1) and $\mathcal{A}$ is a characteristic set of P, then the σ^*-dimension polynomial of the system is determined by the leaders of elements of $\mathcal{A}$. Therefore, the strength of a prime system of difference equations is determined by a characteristic set of the associated σ^*-ideal in the ring of σ^*-polynomials.

An autoreduced subset $\mathcal{A}$ of R consisting of quasi-linear σ^*-polynomials is called *coherent* if it satisfies the following two conditions: (i) If $A \in \mathcal{A}$ and $\gamma \in \Gamma$, then γA reduces to zero modulo $\mathcal{A}$; (ii) If $A, B \in \mathcal{A}$ and $v = \gamma_1 u_A = \gamma_2 u_B$ is a common transform of u_A and u_B, then the σ^*-polynomial $(\gamma_2 I_B)(\gamma_1 A) - (\gamma_1 I_A)(\gamma_2 B)$ reduces to zero modulo $\mathcal{A}$.

The following two statements are the main results that allow one to evaluate the Einstein's strength of difference equations that arise from difference schemes for some chemical reaction-diffusion equations arising in many problems of transfusion, see [2].

Theorem 1. *If a characteristic set $\mathcal{A}$ of some σ^*-ideal in R consists of quasi-linear σ^*-polynomials, then $\mathcal{A}$ is a coherent autoreduced set. Conversely, if $\mathcal{A}$ is a coherent autoreduced set consisting of quasi-linear σ^*-polynomials, then it is a characteristic set of $[\mathcal{A}]^*$.*

Theorem 2. *Let $\preccurlyeq$ be a preorder on R such that $A_1 \preccurlyeq A_2$ iff u_{A_2} is a transform of u_{A_1}. Let A be a quasi-linear σ^*-polynomial and $\Gamma A = \{\gamma A \,|\, \gamma \in \Gamma\}$. Then the σ^*-ideal $[\mathcal{A}]^*$ is prime and all minimal (with respect to $\preccurlyeq$) elements of ΓA form a characteristic set of $[\mathcal{A}]^*$.*

Using the last two theorems and the expression of the σ^*-dimension polynomial given in [3, Theorem 6.4.8], we obtain σ^*-dimension polynomials that express the Einstein's strength of difference schemes for some quasi-linear reaction-diffusion PDEs (e. g., the Murray's equation and its particular cases), the system of PDEs

of chemical reaction kinetics with the diffusion phenomena and the mass balance PDEs of chromatography. The results of the corresponding computations allow one to do comparative analysis of alternative difference schemes from the point of view of their strength.

This work was supported by the NSF grant CCF-1714425.

References

[1] A. EINSTEIN, *The Meaning of Relativity. Appendix II (Generalization of gravitation theory)*, 4th ed. Princeton, 1953.

[2] A. A. EVGRAFOV, Standardization and Control of the Quality of Transfusion Liquids. *Ph. D. Thesis. Sechenov First Moscow State Medical University*. Moscow, 1998.

[3] M. V. KONDRATEVA; A. B. LEVIN; A. V. MIKHALEV; E. V. PANKRATEV, *Differential and Difference Dimension Polynomials*. Kluwer Acad. Publ., Dordrecht, 1998.

[4] A. B. LEVIN, *Difference Algebra*. Springer, New York, 2008.

[1]Department of Analytical, Physical and Colloid Chemistry
Sechenov First Moscow State Medical University
Moscow 119991, Russia
afkx_farm@mail.ru

[2]Department of Mathematics
The Catholic University of America
Washington, D.C. 20064, USA
levin@cua.edu

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Computation of differential Chow forms for ordinary prime differential ideals

Wei Li[1], **Ying-Hong Li**[1]

The differential Chow form is an important associated form for a prime differential ideal or an order-unmixed differential cycle [1]. For example, it can characterize invariants of its corresponding prime differential ideal, such as the differential dimension, order, leading differential degree and differential degree. So it is desirable to devise efficient algorithms to compute the differential Chow form. In this talk, we propose algorithms for computing differential Chow forms for ordinary prime differential ideals which are given by characteristic sets. The algorithms are based on an optimal bound for the order of a prime differential ideal in terms of a characteristic set under an arbitrary ranking, which shows the Jacobi bound conjecture holds in this case. That is, $\mathrm{ord}(\mathrm{sat}(\mathcal{A})) \leq \mathrm{Jac}(\mathcal{A})$. Apart from the order bound, we also give a Bézout type degree bound for the differential Chow form. The computational complexity of the algorithms is single exponential in terms of the Jacobi number, the maximal degree of the differential polynomials in a characteristic set, and the number of variables.

Keywords: Differential Chow form, Jacobi bound, Single exponential algorithm

References

[1] X.S. GAO, W. LI, C.M. YUAN, Intersection Theory in Differncial Algebraic Geometry: Generic Intersections and the Differencial Chow Form. *Trans. Amer. Math. Soc.*, **365**(9), 4575-4632 (2013).

[2] W. LI AND Y.H. LI, Computation of differential Chow forms for ordinary prime differential ideals. *Advances in Applied Mathematics*, **72**, 77-112 (2016).

[1]KLMM, Academy of Mathematics and Systems Science
Chinese Academy of Sciences
Beijing 100190, China
liwei@mmrc.iss.ac.cn
liyinghong10@mails.ucas.ac.cn

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Group Classification of ODEs: a Challenge to Differential Algebra?

Dmitry Lyakhov[1], **Vladimir Gerdt**[2], **Dominik Michels**[3]

One of the most prominent application of differential algebra is algebraic analysis of determining system of partial differential equations for infinitesimal symmetry generators. It provides receipts and software tools to compute the integrability conditions, to simplify (e.g. to interreduce) the system, to determine a dimension of its space, to construct the abstract Lie algebra for the symmetry generators, to apply the Lie symmetry algebra for ordinary differential equations (ODEs) to detect their linearizability [1] by point transformations. The problem of group classification for differential equations was first posed by the Norwegian mathematician Sophus Lie, the inventor of the concept and theory of continuous groups and their application to differential equations [2]. Lie began to solve the group classification problem for the second-order ordinary equation $y'' = f(x, y, y')$ and proved that this class of equations admits no more than an eight-parameter transformation group on the plane with the maximum size of the group is reached iff the equation is linear or equivalent to the linear one. The Russian mathematician Lev Ovsyannikov [3] proposed the equivalence transformation (ET) method for group classification and later [4] applied it to the ODE of form $y'' = f(x, y)$. The ET method is based on the fact that equivalent equations admit similar groups and ET is a similarity transformation. The problem of group classification admits reformulation as an elimination problem in differential algebra. However, even reproduction of the results, obtained in [4] by hand computation, seems to be too hard for the modern differential elimination tools. In the talk we discuss both the pure mathematical and computational issues of the group classification for ODEs.

Keywords: Differential Algebra, Group Classification, Ordinary Differential Equations

References

[1] D. LYAKHOV, V. GERDT, D. MICHELS, *Algorithmic Verification of Linearizability for Ordinary Differential Equations*. Proceedings of ISSAC 2017, ACM Press, 2017, pp.285–292. arXiv:math.CA/1702.03829

[2] S. Lie. *Klassifikation und Integration von gewöhnlichen Differentialgleichungen zwischen x, y, die eine Gruppe von Transformationen gestatten*. III. Archiv for

Matematik og Naturvidenskab, 8(4), 1883, 371–458. Reprinted in Lie's Gessammelte Abhandlungen, 5, paper XIY, 1924, 362–427.

[3] L. OVSYANNIKOV, *Group Analysis of Differential Equations*. Academic Press, New York, 1992.

[4] L. OVSYANNIKOV, *Group Classification of Equations of the Form* $y'' = f(x, y)$. Journal of Applied Mechanics and Technical Physics, Vol. 45, No. 2, pp. 153–157, 2004.

[1]Visual Computing Center
King Abdullah University of Science and Technology
Thuwal, Saudi Arabia
dmitry.lyakhov@kaust.edu.sa

[2]Laboratory of Information Technologies
Joint Institute for Nuclear Research
Dubna, Russia
gerdt@jinr.ru

[1]Visual Computing Center
King Abdullah University of Science and Technology
Thuwal, Saudi Arabia
dominik.michels@kaust.edu.sa

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Power series solutions of systems of nonlinear PDEs

Daniel Robertz[1]

One of the first existence theorems for a large class of PDEs is the Cauchy-Kovalevskaya Theorem [5]. In work of C. Méray and C. Riquier in the second half of the 19th century a generalization of the Cauchy-Kovalevskaya Theorem was obtained. Riquier's Existence Theorem asserts the existence of analytic solutions for the class of orthonomic and passive systems of PDEs [7, Chap. VIII]. J. M. Thomas [9] showed that polynomially nonlinear systems of PDEs can be decomposed into finitely many so-called simple differential systems, each of which can be solved for the highest ranked derivatives to obtain orthonomic and passive systems. Building also on work by M. Janet [4], the algorithmic details of the Thomas decomposition method have been recently developed [1], [2], [6], [8].

In this talk we explain how the differential Thomas decomposition can be used to find all power series solutions around sufficiently generic points of a system of nonlinear partial differential equations. Further applications of the Maple package for computing Thomas decompositions [3], e.g. to differential elimination, are demonstrated as well. The talk is based on joint work with Vladimir Gerdt and Markus Lange-Hegermann.

Keywords: completion to involution, Thomas decomposition, differential elimination

References

[1] T. BÄCHLER; V. P. GERDT; M. LANGE-HEGERMANN; D. ROBERTZ, Algorithmic Thomas Decomposition of Algebraic and Differential Systems. *J. Symbolic Comput.* **47**(10), 1233–1266 (2012).

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

[3] V. P. GERDT; M. LANGE-HEGERMANN; D. ROBERTZ, The MAPLE package TDDS for computing Thomas decompositions of systems of nonlinear PDEs. Submitted for publication, `http://arxiv.org/abs/1801.09942`.

[4] M. JANET, Les systèmes d'équations aux dérivées partielles. *J. de Math.,* 8^e *série* **3**, 65–151 (1920).

[5] S. KOWALEVSKY, Zur Theorie der partiellen Differentialgleichung. *J. Reine & Angewandte Mathematik* **80**, 1–32 (1875).

[6] M. LANGE-HEGERMANN, *Counting Solutions of Differential Equations*. PhD thesis, RWTH Aachen University, Germany, 2014, available online at `http://publications.rwth-aachen.de/record/229056`.

[7] J. F. RITT, *Differential Algebra*. Vol. XXXIII of American Mathematical Society Colloquium Publications, American Mathematical Society, New York, 1950.

[8] D. ROBERTZ, *Formal Algorithmic Elimination for PDEs*. Vol. 2121 of Lecture Notes in Mathematics, Springer, Cham, 2014.

[9] J. M. THOMAS, *Differential Systems*. Vol. XXI of American Mathematical Society Colloquium Publications, American Mathematical Society, New York, 1937.

[1]School of Computing, Electronics and Mathematics
Plymouth University,
2-5 Kirkby Place, Drake Circus, Plymouth PL4 8AA, UK
`daniel.robertz@plymouth.ac.uk`

S7

Algebraic and Algorithmic Aspects of Differential and Integral Operators

The algebraic/symbolic treatment of differential equations is a flourishing field, branching out in a variety of subfields committed to different approaches. In this session, we want to give special emphasis to the operator perspective of both the underlying differential operators and various associated integral operators (e.g. as Green's operators for initial/boundary value problems).

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

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

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

The Jacobian algebras, their ideals and automorphisms

V. V. Bavula[1]

The talk is about general properties of the Jacobian algebras (in arbitrary many variables), classifications of their ideals, an explicit description of their groups of automorphisms. Explicit values of their global and weak dimensions are found.

Keywords: Jacobian algebra, group of automorphisms, global and weak dimension

[1]School of Mathematics and Statistics,
University of Sheffield, UK
v.bavula@sheffield.ac.uk

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

On the Parameter Estimation Problem for Integro-Differential Models*

François Boulier[1]

This talk summarizes a joint work with modelers and biologists [2]. It deals with the parameter estimation problem for dynamical systems presented by explicit systems of polynomial integro-differential equations (IDE).

Models formulated by means of IDE are very interesting because they are much more expressive than their ODE counterparts: they naturally permit to express delays (IDE are viewed as continuous delay differential equations in [9]), to take into account the age of populations (typical motivation for integral equations in population dynamics), to incorporate curves obtained by interpolating experimental data as integral kernels (an important feature for modeling processes interacting with complicated environment) and to handle non smooth (e.g. piecewise defined) inputs. See [6] and references therein.

The rest of this abstract is essentially borrowed from the introduction of [2].

IDE modeling raises, in turn, the problem of estimating parameters from experimental data. This talk focuses on a particular method, called the "input-output (IO) ideal" method, which is available in the nonlinear ODE case. Its principle consists in computing an equation (called the "IO equation") which is a consequence of the model equations and only depends on the model inputs, outputs and parameters. In the nonlinear ODE case, it is known since [8] that it can serve to decide the identifiability property of the model. It is known since [7] that it can also be used to determine a first guess of the parameters from experimental data. This first guess may then be refined by means of a nonlinear fitting algorithm (of type Levenberg-Marquardt) which requires many different numerical integrations of the model.

Designing analogue theories and algorithms in the IDE case is almost a completely open problem. The talk presents two contributions:

1. a symbolic method for computing an IO equation from a given nonlinear IDE model. This method is incomplete but it is likely to apply over an important class of models that are interesting for modelers. It relies on the elimination theory for differential algebra [4, 5] and on an algorithm for integrating differential fractions [3];

*This work has been supported by the bilateral project ANR-17-CE40-0036 and DFG-391322026 SYMBIONT

2. an algorithm for the numerical integration of IDE systems, implemented within a new open source C library [1]. The library does not seem to have any available equivalent. Our algorithm is an explicit Runge-Kutta method which is restricted to Butcher tableaux specifically designed in order to avoid solving integral equations at each step.

Keywords: nonlinear integro-differential, input-output equation, parameter estimation, numerical integration

References

[1] FRANÇOIS BOULIER AND AL, *BLINEIDE*. `http://cristal.univ-lille.fr/~boulier/BLINEIDE`.

[2] FRANÇOIS BOULIER, HÉLÈNE CASTEL, NATHALIE CORSON, VALENTINA LANZA, FRANÇOIS LEMAIRE, ADRIEN POTEAUX, ALBAN QUADRAT, AND NATHALIE VERDIÈRE, *Symbolic-Numeric Methods for Nonlinear Integro-Differential Modeling*. Submitted to CASC (2018), `http://hal.archives-ouvertes.fr/hal-01765409`.

[3] FRANÇOIS BOULIER, JOSEPH LALLEMAND, FRANÇOIS LEMAIRE, GEORG REGENSBURGER, AND MARKUS ROSENKRANZ, *Additive normal forms and integration of differential fractions*. *JSC* **77**, 77-38 (2016).

[4] FRANÇOIS BOULIER, DANIEL LAZARD, FRANÇOIS OLLIVIER, AND MICHEL PETITOT, *Representation for the radical of a finitely generated differential ideal*. In *Proceedings of ISSAC'95*, Montreal, 1995.

[5] FRANÇOIS BOULIER, DANIEL LAZARD, FRANÇOIS OLLIVIER, AND MICHEL PETITOT, *Computing representations for radicals of finitely generated differential ideals*. *AAECC* **20**(1), 73–121 (2009).

[6] FRANÇOIS BOULIER, FRANÇOIS LEMAIRE, MARKUS ROSENKRANZ, ROSANE USHIROBIRA, AND NATHALIE VERDIÈRE, *On Symbolic Approaches to Integro-Differential Equations*. In *Advances in Delays and Dynamics* (2017), `https://hal.archives-ouvertes.fr/hal-01367138`.

[7] LILIANNE DENIS-VIDAL, GHISLAINE JOLY-BLANCHARD, AND CÉLINE NOIRET, *System identifiability (symbolic computation) and parameter estimation (numerical computation)*. In *Numerical Algorithms* **34** 282–292 (2003).

[8] LENNART LJUNG AND TORKEL GLAD. *On global identifiability for arbitrary model parametrisations*. *Automatica* **30** 265–276 (1994).

[9] WIKIPEDIA. *Delay Differential Equations*. https://en.wikipedia.org/wiki/Delay_differential_equation.

[1]CRIStAL - UMR 9189
University of Lille, CNRS, Centrale Lille, Inria
Francois.Boulier@univ-lille.fr

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Parametric b-functions for some hypergeometric ideals*

Francisco-Jesús Castro-Jiménez[1], **Helena Cobo Pablos**[1]

We denote by $D := \mathbb{C}[x_1, \ldots, x_n, \partial_1, \ldots, \partial_n]$ the Weyl algebra over the field $\mathbb{C}$.

The aim of this note is to study the b–function associated with a class of hypergeometric ideals $H_A(\beta) \subseteq D$ following [9, Section 5.1]. Let us recall the definition of $H_A(\beta)$. Given $A = (a_{ij})$ a $d \times n$ matrix of rank d with integer coefficients, we first consider the associated toric ideal $I_A \subset \mathbb{C}[\partial] := \mathbb{C}[\partial_1, \ldots, \partial_n]$

$$I_A := \mathbb{C}[\partial]\{\partial^u - \partial^v \mid u, v \in \mathbb{N}^n, Au = Av\}.$$

Moreover we consider the Euler operators, for $1 \leq i \leq d$

$$E_i = a_{i1}x_1\partial_1 + \cdots + a_{in}x_n\partial_n.$$

Then for any parameter vector $\beta \in \mathbb{C}^d$ the hypergeometric ideal is defined as

$$H_A(\beta) = D \cdot I_A + \sum_{1 \leq i \leq d} D(E_i - \beta_i).$$

Given a holonomic left ideal I in D and a nonzero weight vector $\omega \in \mathbb{R}^n$, we denote $in_{(-\omega,\omega)}(I) \subset D$ the initial ideal of I with respect to the filtration $(F_p)_{p\in\mathbb{R}}$ induced on D by the vector $(-\omega, \omega) \in \mathbb{R}^{2n}$. The $\mathbb{C}$–vector space F_p is defined as follows:

$$F_p := \mathbb{C}\{x^\alpha\partial^\beta \mid -\omega\alpha + \omega\beta \leq p\} \quad \text{for } p \in \mathbb{R}.$$

Kashiwara has introduced in (*On the Holonomic Systems of Linear Differential Equations, II.* Inventiones Math. 49, 121–135, 1978) the b–function $b_{I,\omega}(s)$ associated with the pair (I, ω), as the monic generator of the ideal

$$in_{(-\omega,\omega)}(I) \cap \mathbb{C}[s] \tag{1}$$

where $s := \sum_{i=1}^n \omega_i x_i \partial_i$. It is proven in *loc. cit. Theorem 2.7* that the ideal in (1) is nonzero. In this note we follow the presentation and notations of [9, §5] on this subject.

The polynomial $b_{I,\omega}(s)$ is called the b–function of the holonomic ideal $I \subset D$ with respect to the weight vector ω.

Previous b-functions are closely related to the classical notion of Bernstein polynomial (also called Bernstein-Sato polynomial) $b_f(s)$ associated with a given nonzero

*Partially supported by MTM2013-40455-P, MTM2016-75024-P and Feder

polynomial $f \in \mathbb{C}[x]$ (see e.g. [9, Lemma 5.3.11]). Bernstein polynomials have been introduced in [2] and [8] and represent fundamental invariants in singularity theory. There are several algorithms for computing Bernstein polynomials. Some of them are described in [5], [6], [4], and [1]. These and other algorithms have been implemented in the computer algebra systems `Asir`, `Macaulay2` and `Singular` among others. Nevertheless, in practice $b_f(s)$ is hard to compute even in the case of a polynomial f in two variables. In [3] the authors propose the algorithm `checkRoot` which, given a rational number α checks if it is a root of the Bernstein polynomial $b_f(s)$, and computes its multiplicity.

We simply denote $b_{\omega,\beta}(s) := b_{H_A(\beta),\omega}(s)$. We refer to [9] for the main results on hypergeometric ideals and the corresponding b–functions $b_{\omega,\beta}(s)$ *for generic parameters* w *and* β (see below for details). In [7] the authors describe bounds for the roots of $b_{\omega,\beta}(s)$.

In this paper we restrict ourselves to matrices of the form $A = (1, p, q)$ with integers $1 < p < q$ and p and q coprime. The first step is to describe the Gröbner fan of the toric ideal I_A, as defined in (T. Mora; L. Robbiano, The Gröbner fan of an ideal. *J. Symbolic Comput.* **6**(2-3) 183–208 (1988)) and in (B. Sturmfels, *Gröbner bases and convex polytopes*. University Lecture Series, 8. Providence RI, 1995.) We define a finite family of disjoint regions $R_i^{(k)} \subset \mathbb{R}^3$ which are the intersection of two half-spaces with the line $(1, p, q)\mathbb{R}$ in common (see Example). The possible integers k and i depend on the extended Euclidean division of q over p. We prove an equality $\mathbb{R}^3 = \bigcup_{i,k} \overline{R_i^{(k)}}$ such that for each $\omega \in R_i^{(k)}$, the initial ideal $in_\omega(I_A)$ is a monomial ideal and it is independent of ω.

In [9, Proposition 5.1.9.] there is a description of $b_{\omega,\beta}(s)$ for Zariski generic β and generic ω In (M.C. Fernández-Fernández, *Soluciones Gevrey de sistemas hipergeométricos asociados a una curva monomial lisa.* DEA, U. Sevilla, 2008.), the polynomial $b_{\omega,\beta}(s)$ is described for $\omega = (1, 0, 0)$ and β generic. Our main result is:

Theorem 3. *Given $R_i^{(k)}$, a facet of the Gröbner fan of I_A, there is a proper Zariski closed set $C_i^{(k)} \subset R_i^{(k)}$ such that if $\omega \in R_i^{(k)} \setminus C_i^{(k)}$ and β is generic the b–function is*

$$b_{\omega,\beta}(s) = \prod_{\alpha \in F_i^{(k)}} (s - \alpha)$$

for certain finite set $F_i^{(k)} \subseteq \mathbb{C}$. Moreover, if $\omega \in C_i^{(k)}$ or β is non-generic, the right hand side of previous equality gives a multiple of the b–function.

The set $F_i^{(k)}$ is explicitly described in terms of standard monomials of $in_{(-\omega,\omega)}(H_A(\beta))$. In the following example we sum up our results.

Example. Consider the matrix $A = (1, 3, 5)$. The Gröbner fan of $I_A \subset \mathbb{C}[\partial_x, \partial_y, \partial_z]$ consists of seven facets. Let us focus in one of them, namely $R_1^{(2)} = \{\omega \in \mathbb{R}^3 \mid 2\omega_1 +$

$\omega_2 > \omega_3, \omega_1 + 3\omega_2 < 2\omega_3\}$. For any $\omega \in R_1^{(2)}$

$$in_\omega(I_A) = D\left(\partial_x^3, \partial_x^2\partial_y, \partial_x\partial_z, \partial_z^2\right).$$

Any complex number $\beta \neq 2$ is generic, and we have that

$$in_{(-\omega,\omega)}(H_A(\beta)) = D\left(\partial_x^2, \partial_x\partial_z, \partial_z^2, E - \beta\right).$$

We have $C_1^{(2)} = R_1^{(2)} \cap \{3\omega_1 + 4\omega_2 = 3\omega_3\}$. The b–function for $\omega \in R_1^{(2)} \setminus C_1^{(2)}$ and $\beta \neq 2$ is

$$b_{\omega,\beta}(s) = (s - \frac{\beta}{3}\omega_2)(s - \omega_1 - \frac{\beta-1}{3}\omega_2)(s - \frac{\beta-5}{3}\omega_2 - \omega_3).$$

If $\omega \in C_1^{(2)}$ and $\beta \neq 2$, the polynomial

$$(s - \frac{\beta}{3}\omega_2)(s - \omega_1 - \frac{\beta-1}{3}\omega_2)$$

is a multiple of the b–function. With `Singular` we check that in this case we obtain the true b–function and not just a multiple. If $\omega \in R_1^{(2)}$ but $\beta = 2$ we have the following multiple of the b–function:

$$\begin{cases} (s - \frac{2}{3}\omega_2)(s - \omega_1 - \frac{1}{3}\omega_2)(s - 2\omega_1)(s + \omega_2 - \omega_3) & \text{if } \omega \notin C_1^{(2)} \\ (s - \frac{2}{3}\omega_2)(s - \omega_1 - \frac{1}{3}\omega_2)(s - 2\omega_1) & \text{otherwise.} \end{cases}$$

Again, with `Singular` we check that this is indeed $b_{\omega,2}(s)$. However, if we consider the region $R_2^{(2)} = \{\omega \in \mathbb{R}^3 \mid \omega_1 + 3\omega_2 > 2\omega_3, 3\omega_3 > 5\omega_2\}$, we have $\beta = 1, 2, 4, 7$ as non-generic values, and for $\omega \in R_2^{(2)}$ and $\beta = 2$ we give a polynomial with five roots, and only four of them are the roots of $b_{\omega,2}(s)$.

If $\omega \in \mathbb{R}^3 \setminus \bigcup_{i,k} R_i^{(k)}$ the study of $b_{\omega,\beta}(s)$ is a work in progress.

Keywords: b–function, hypergeometric ideal.

References

[1] D. ANDRES, *Noncommutative Computer Algebra with Applications in Algebraic Analysis*. Dissertation, Universität Aachen, 2014.

[2] I.N. BERNSTEIN, Analytic continuation of generalized functions with respect to a parameter. *Funkcional. Anal. i Priložen* **6**(4), 26–40 (1972).

[3] V. LEVANDOVSKYY; J. MARTÍN-MORALES, Algorithms for checking rational roots of b-functions and their applications. *J. Algebra* **352** 408–429 (2012).

[4] M. NORO, An efficient modular algorithm for computing the global b-bunction. In *Mathematical software (Beijing 2002)*, 147–157. World Sci. Publ., River Edge, NJ, 2002.

[5] T. OAKU, An algorithm of computing b–functions. *Duke Math. J.* **87**(1), 115–132 (1997).

[6] T. OAKU, Regular b–functions of D-modules. *J. Pure Appl. Algebra* **213**, 1545–1557 (2009).

[7] T. REICHELT; CH. SEVENHECK; U. WALTHER, On the b–functions of hypergeometric systems. *Int. Math. Res. Not.*, doi.org/10.1093/imrn/rnx039, 2017.

[8] M. SATO, Theory of prehomogeneous vector spaces (algebraic part)–Notes by T. Shintani. Translated from the Japanese by M. Muro. *Nagoya Math. J.*, **120**, 1–34 (1990).

[9] M. SAITO; B. STURMFELS; N. TAKAYAMA, *Gröbner deformations of hypergeometric differential equations.* Springer-Verlag, Berlin, (2000).

[1]Departamento de Álgebra and IMUS. Universidad de Sevilla
Campus Reina Mercedes
41012 Sevilla (Spain)
castro@us.es, helenacobo@gmail.com

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Reduction operators and completion of linear rewriting systems

Cyrille Chenavier[1]

In rewriting theory, the confluence property guarantees the coherence of calculi. In this talk, we study the confluence property for linear rewriting systems defined by reduction operators. We use this approach to provide a lattice description of obstructions to confluence. We deduce lattice formulations of the completion procedure as well as a method for extending linear rewriting systems so that they become confluent.

Keywords: Reduction operators, Lattice structure, Confluence, Completion procedure

[1]Computer science
Université Paris-Est Marne-la-Vallée
Laboratoire d'informatique Gaspard Monge
Université Paris-Est Marne-la-Vallée
Cité Descartes, 5 Boulevard Descartes, Champs-sur-Marne
77454 Marne-la-Vallée cedex 2
cyrille.chenavier@u-pem.fr

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Observability and orders of derivatives of data

Sette Diop[1]

Observability of nonlinear systems has been approached using differential algebraic geometry with quite interesting breakthroughs in this systems theory notion. Among detailed aspects to be studied is the relationship between observability of, say z, and the minimum order of derivatives of data. This relationship is an ingredient in the design and the complexity of observers. This talk will give new insights in this topic.

Keywords: Observability, systems theory, differential algebra

[1]Laboratoire des Signaux & Systèmes,
France
diop@l2s.centralesupelec.fr

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Effective criterion to test differential transcendence of special functions.

Carlos Arreche[1], **Thomas Dreyfus**[2], **Julien Roques**[3]

Consider a field $\mathbf{k}$ equipped with an automorphism ϕ. Typical examples are

- $\mathbf{k} = \mathbb{C}^{\mathbb{Z}}$, $\phi(u_n) := (u_{n+1})$;
- $\mathbf{k} = \mathbb{C}(x)$, $\phi f(x) := f(x+1)$;
- $\mathbf{k} = \mathbb{C}(x)$, $\phi f(x) := f(qx)$, $q \in \mathbb{C}^*$;
- $\mathbf{k} = \cup_{\ell \in \mathbb{N}^*} \mathbb{C}(x^{1/\ell})$, $\phi f(x) := f(x^p)$, $p \in \mathbb{N}^*$.

A difference equation is a linear equation of the form

$$a_0 y + \cdots + a_n \phi^n(y) = 0,$$

with $a_0, \ldots, a_n \in \mathbf{k}$. The difference Galois theory, see [1], attaches to such equation a linear algebraic subgroup of $\mathrm{GL}_n(\mathbb{C})$ that measures the algebraic relations among the solutions of the difference equation. More recently, it has been developed in [2] a Galois theory that aims at understanding the algebraic and differential relations among the solutions of the difference equation

The goal of this talk is to give explicit and computable criteria to ensure that a solutions of an order two difference equation does not satisfy any algebraic differential equations in coefficients in $\mathbf{k}$. We apply this criterion to the elliptic analogue of the hypergeometric functions.

Keywords: Difference Galois theory

References

[1] VAN DER PUT, MARIUS AND SINGER, MICHAEL F, *Galois theory of difference equations*.

[2] HARDOUIN, CHARLOTTE AND SINGER, MICHAEL F, Differential Galois theory of linear difference equations. *Mathematische Annalen*.

[1]The University of Texas at Dallas,
Mathematical Sciences FO 35,
800 West Campbell Road, Richardson, TX 75024, USA
arreche@utdallas.edu

[2]Institut de Recherche Mathématique Avancée,
U.M.R. 7501 Université de Strasbourg et C.N.R.S.
7, rue René Descartes 67084 Strasbourg, FRANCE
dreyfus@math.unistra.fr

[3]Institut Fourier,
Université Grenoble 1, CNRS UMR 5582,
100 rue des Maths, BP 74, 38402 St Martin d'Hères
Julien.Roques@ujf-grenoble.fr

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Rota's Classification Problem, Rewriting Systems and Gröbner-Shirshov Bases

Li Guo[1]

Throughout the history, mathematical objects are often understood through studying operators defined on them. Well-known examples include Galois theory where a field is studied by its automorphisms (the Galois group), and analysis and geometry where functions and manifolds are studied through their derivations, integrals and related vector fields.

A long time ago, Rota raised the question of identifying all the identities that could be satisfied by a linear operator defined on algebras. We will discuss some recent progress on understanding and solving Rota's Problem by the methods of rewriting systems and Gröbner-Shirshov bases.

This is joint work with Xing Gao, William Sit, Ronghua Zhang and Shanghua Zheng.

Keywords: Linear operators, Gröbner-Shirshov bases, rewriting systems

[1]Rutgers University,
Newark, New Jersey, USA
liguo@rutgers.edu

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Symbolic computation for integro-differential-time-delay operators with matrix coefficients

Thomas Cluzeau[1], **Jamal Hossein Poor**[2], **Alban Quadrat**[3], **Clemens G. Raab**[4], **Georg Regensburger**[5]

In order to facilitate symbolic computations with systems of linear functional equations, we require an algebraic framework for such systems which enables effective computations in corresponding rings of operators. We briefly explain the recent developed tensor approach from scalar equations [1] to the matrix case [2], by allowing noncommutative coefficients. Noncommutative coefficients even allow to handle systems of generic size. Normal forms are a key ingredient for computing with operators and rely on a confluent reduction system.

The tensor approach is flexible enough to cover many operators, like integral operators, that do not fit the well established framework of skew-polynomials. For instance, it can be used to construct the ring of integro-differential operators with linear substitutions (IDOLS) having (noncommutative) matrix coefficients, containing the ring of integro-differential-time-delay operators. In the `Mathematica` package `TenRes` we provide support for tensor reduction systems [3]. In addition, we implement the ring of IDOLS and corresponding normal forms. We illustrate how, by elementary computations in this framework, results like the method of steps can be found and proven in an automated way. We also apply normal forms of IDOLS to partly automatize certain computations related to differential time-delay systems, e.g. Artstein's transformation [4] and its generalization [5].

This work is supported by PHC AMADEUS project no. 35602WA, WTZ project no. FR10/2016, and FWF project no. P27229.

Keywords: integro-differential operators with linear substitutions, Artstein's reduction, algebraic analysis approach to linear systems theory

References

[1] J. Hossein Poor; C. G. Raab; G. Regensburger, *Algorithmic operator algebras via normal forms for tensors*. In *Proceedings of ISSAC 16*, pp. 397–404, 2016.

[2] J. Hossein Poor; C. G. Raab; G. Regensburger, *Algorithmic operator algebras via normal forms in tensor rings, 33 pages*. Journal of Symbolic Computation, **85**, pp. 247–274, 2018.

[3] J. Hossein Poor; C. G. Raab; G. Regensburger *Normal forms for operators via Gröbner bases in tensor algebras*, In *Proceedings of ICMS 2016*, volume 9725 of *LNCS*. Springer, pp. 505–513, 2016.

[4] A. QUADRAT, *A constructive algebraic analysis approach to Artstein's reduction of linear time-delay systems*, In *IFAC-PapersOnLine*, 48 (12), pp. 209–214, 2015.

[5] T. CLUZEAU; J. HOSSEIN POOR; A. QUADRAT; C.G. RAAB; G. REGENSBURGER, *Symbolic computation for integro-differential-time-delay operators with matrix coefficients*, 6 pages, 2018, submitted.

[1]XLIM UMR 7252
University of Limoges
87060 Limoges, France,
thomas.cluzeau@unilim.fr

[2]RICAM,
Austrian Academy of Sciences
4040 Linz, Austria
jamal.hossein.poor@ricam.oeaw.ac.at

[3]INRIA Lille-Nord Europe, GAIA team
59650 Vileneuve d'Ascq, France,
alban.quadrat@inria.fr.

[4,5]Algebra department
Johannes Kepler University Linz
4040 Linz, Austria,
clemens.raab@jku.at,
georg.regensburger@jku.at.

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Low-Order Recombinations of C-Finite Sequences

Maximilian Jaroschek[1,2], **Manuel Kauers**[1], **Laura Kovács**[2]

One of the central open problems for C-finite sequences, that is sequences that admit a linear recurrence equation with constant coefficients, is the Skolem problem, which asks if a given sequence includes the term 0. Special instances for which an answer can be given algorithmically include the case where there exists an annihilating recurrence of order less than or equal to 4. The Skolem problem is of particular interest in program verification, as the values of loop variables in practice often describe C-finite sequences. We investigate how to combine these C-finite sequences via term-wise multiplication and addition so that the resulting sequences admit recurrences of low order. These combinations then can be used as inequality loop invariants in automatic program analysis.

Keywords: C-finite Sequences, Skolem Problem, Invariant Generation

[1]Institute for Algebra
Johannes Kepler University Linz
Altenberger Str. 69
4040 Linz, Austria
maximilian@mjaroschek.com
manuel.kauers@jku.at

[2]Institute for Logic and Computation
Technical University Vienna
Favoritenstr. 9–11
1040 Vienna, Austria
lkovacs@forsyte.at

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Some Properties and Invariants of Multivariate Difference-Differential Dimension Polynomials

Alexander Levin[1]

Multivariate dimension polynomials associated with finitely generated differential and difference field extensions arise as natural generalizations of the univariate differential and difference dimension polynomials defined respectively in [1] and [2]. It turns out, however, that they carry more information about the corresponding extensions than their univariate counterparts (see [3, Theorem 4.2.17] and [4]). In this presentation we extend the known results on multivariate dimension polynomials to the case of difference-differential field extensions with arbitrary partitions of sets of basic operators. We also describe some properties of multivariate dimension polynomials and their invariants. The following is the outline of the talk.

Let K be a difference-differential field, $\mathrm{Char}\, K = 0$, and let $\Delta = \{\delta_1, \ldots, \delta_m\}$ and $\sigma = \{\alpha_1, \ldots, \alpha_n\}$ be basic sets of derivations and automorphisms of K, respectively. Below we often use the prefix Δ-σ- instead of "difference-differential". Suppose that the sets Δ and σ are represented as unions of disjoint subsets: $\Delta = \cup_{i=1}^{p} \Delta_i$ and $\sigma = \cup_{j=1}^{q} \sigma_j$ where $\mathrm{Card}\, \Delta_i = m_i$ $(1 \leq i \leq p)$ and $\mathrm{Card}\, \sigma_i = n_i$ $(1 \leq i \leq q)$. Let Λ denote the free commutative semigroup of all power products of the form $\lambda = \delta_1^{k_1} \ldots \delta_m^{k_m} \alpha_1^{l_1} \ldots \alpha_n^{l_n}$ where $k_\mu \in \mathbb{N}$, $l_\nu \in \mathbb{Z}$ and for every such λ, let

$$\mathrm{ord}_{\Delta_i} \lambda = \sum_{\mu \in \Delta_i} k_\mu \ \text{ and } \ \mathrm{ord}_{\sigma_j} \lambda = \sum_{\nu \in \sigma_j} |l_\nu|$$

$(1 \leq i \leq p, 1 \leq j \leq q)$. Furthermore, for any $(r_1, \ldots, r_{p+q}) \in \mathbb{N}^{p+q}$, let $\Lambda(r_1, \ldots, r_{p+q}) = \{\lambda \in \Lambda \,|\mathrm{ord}_{\Delta_i} \lambda \leq r_i$ for $i = 1, \ldots, p$ and $\mathrm{ord}_{\sigma_j} \lambda \leq r_{p+j}$ for $j = 1, \ldots, q\}$. The following theorem generalizes the main result of [4].

Theorem 4. *Let $L = K\langle \eta_1, \ldots, \eta_s \rangle$ be a Δ-σ-field extension generated by a set $\eta = \{\eta_1, \ldots, \eta_s\}$. Then there exists a polynomial $\Phi_\eta \in \mathbb{Q}[t_1, \ldots, t_{p+q}]$ (called the Δ-σ-dimension polynomial of the extension L/K) such that*

(i) $\Phi_\eta(r_1, \ldots, r_{p+q}) = \mathrm{tr.deg}_K\, K(\bigcup_{j=1}^{s} \Lambda(r_1, \ldots, r_{p+q})\eta_j)$

for all sufficiently large $(r_1, \ldots, r_{p+q}) \in \mathbb{N}^{p+q}$ (it means that there exist $s_1, \ldots, s_{p+q} \in \mathbb{N}$ such that the equality holds for all $(r_1, \ldots, r_{p+q}) \in \mathbb{N}^{p+q}$ with $r_1 \geq s_1, \ldots, r_{p+q} \geq s_{p+q}$);

(ii) $\deg_{t_i} \Phi_\eta \leq m_i$ *(*$1 \leq i \leq p$*),* $\deg_{t_{p+j}} \Phi_\eta \leq n_j$ *(*$1 \leq j \leq q$*) and* $\Phi_\eta(t_1, \ldots, t_{p+q})$ *can be represented as*

$$\Phi_\eta = \sum_{i_1=0}^{m_1} \ldots \sum_{i_p=0}^{m_p} \sum_{i_{p+1}=0}^{n_1} \ldots \sum_{i_{p+q}=0}^{n_q} a_{i_1 \ldots i_{p+q}} \binom{t_1 + i_1}{i_1} \ldots \binom{t_{p+q} + i_{p+q}}{i_{p+q}}$$

where $a_{i_1 \ldots i_{p+q}} \in \mathbb{Z}$ *and* $2^n \mid a_{m_1 \ldots m_p n_1 \ldots n_q}$.

We sketch the proof of this theorem and present a method of computation of the polynomial Φ_η based on a generalization of the Ritt-Kolchin method of characteristic sets. Furthermore, we determine invariants of a Δ-σ-dimension polynomial, i. e., numerical characteristics of the Δ-σ-field extension that are carried by such a polynomial and that do not depend on the set of Δ-σ-generators this Δ-σ-dimension polynomial is associated with. We also give conditions under which the Δ-σ-dimension polynomial is of the simplest possible form.

Keywords: Difference-differential field extension, Dimension polynomial, Characteristic set

This work was supported by the NSF grant CCF-1714425.

References

[1] E. R. KOLCHIN, The notion of dimension in the theory of algebraic differential equations. *Bull Amer. Math.Soc.*, **70**, 570–573, 1964.

[2] A. B. LEVIN, Characteristic Polynomials of Filtered Difference Modules and Difference Field Extensions. *Russian Math Surv.*, **33**, 165–166, 1978.

[3] A. B. LEVIN, *Difference Algebra*. Springer, New York, 2008.

[4] A. B. LEVIN, Multivariate Difference-Differential Dimension Polynomials and New Invariants of Difference-Differential Field Extensions. *Proceedings of ISSAC 2013*, 267–274. ACM, New York, 2013.

[1]Department of Mathematics
The Catholic University of America
Washington, D.C. 20064, USA
levin@cua.edu

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Computer algebra and the Lanczos problems in arbitrary dimension

J.-F. Pommaret[1]

When $\mathcal{D}$ is a linear partial differential operator of any order, a direct problem is to look for an operator $\mathcal{D}_1$ generating the compatibility conditions (CC) $\mathcal{D}_1\eta = 0$ of $\mathcal{D}\xi = \eta$. We may thus construct a differential sequence with successive operators $\mathcal{D}, \mathcal{D}_1, \mathcal{D}_2, ...$, where each operator is generating the CC of the previous one. Introducing the formal adjoint $ad()$, we have $\mathcal{D}_i \circ \mathcal{D}_{i-1} = 0 \Rightarrow ad(\mathcal{D}_{i-1}) \circ ad(\mathcal{D}_i) = 0$ but $ad(\mathcal{D}_{i-1})$ may not generate all the CC of $ad(\mathcal{D}_i)$. When $D = K[d_1, ..., d_n] = K[d]$ is the (non-commutative) ring of differential operators with coefficients in a differential field K, it gives rise by residue to a differential module M over D. The homological extension modules $ext^i(M) = ext^i_D(M, D)$ with $ext^0(M) = hom_D(M, D)$ only depend on M and are measuring the above gaps, independently of the previous differential sequence.

The purpose of this talk is to explain how to compute extension modules for certain Lie operators involved in the formal theory of Lie pseudogroups in arbitrary dimension n. In particular, we prove that the extension modules highly depend on the Vessiot structure constants c. When one is dealing with a Lie group of transformations or, equivalently, when $\mathcal{D}$ is a Lie operator of finite type, then we shall prove that $ext^i(M) = 0, \forall 0 \leq i \leq n-1$. It will follow that the Riemann-Lanczos and Weyl-Lanczos problems just amount to prove such a result for $i = 2$ and arbitrary n when $\mathcal{D}$ is the Killing or conformal Killing operator. We finally prove that $ext^i(M) = 0, \forall i \geq 1$ for the Lie operator of infinitesimal contact transformations with arbitrary $n = 2p + 1$. Most of these new results have been checked by means of computer algebra.

Keywords: Differential sequence, Variational calculus, Differential constraint, Control theory, Killing operator, Riemann tensor, Bianchi identity, Weyl tensor, Lanczos tensor, Contact transformations, Vessiot structure equations

[1]CERMICS,
Ecole des Ponts ParisTech,
France
jean-francois.pommaret@wanadoo.fr

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Algebraic proofs of operator identities

Jamal Hossein Poor[1], **Clemens G. Raab**[2], **Georg Regensburger**[2]

Many interesting properties of linear operators can be phrased as operator identities, which then can be proven algebraically. In practice, however, linear operators often map between different spaces, then we can no longer add or compose any two such operators. For instance, this already happens with rectangular matrices or with differential operators having rectangular matrix coefficients.

In order to still be able to do meaningful symbolic computations with such operators on the computer, an algebraic framework is needed that deals with the corresponding domains and codomains of operators when adding and multiplying operators. In principle, symbolic computation with such operators (or matrices) would require at each step taking care of the domains and codomains of those operators (or of the formats of the matrices). In contrast, we aim at an a-posteriori justification of an identity, independent of how it was computed algebraically.

In this talk we present first results towards such an algebraic framework based on quivers and noncommutative Gröbner bases, which could be applied to operators with rectangular matrix coefficients. We will also present examples from the theory of generalized inverses using noncommutative Gröbner bases.

Keywords: Linear operators, noncommutative Gröbner bases

References

[1] J. HOSSEIN POOR; C. G. RAAB; G. REGENSBURGER, Algebraic proofs of operator identities. In preparation, 2018.

[1]RICAM
Austrian Academy of Sciences
Altenbergerstr. 69, 4040 Linz, Austria
jamal.hossein.poor@ricam.oeaw.ac.at

[2]Institute for Algebra
Johannes Kepler University Linz
Altenbergerstr. 69, 4040 Linz, Austria
{clemens.raab,georg.regensburger}@jku.at

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Definite Integration of D-finite Functions via Generalized Hermite Reduction

Alin Bostan[1] **Frédéric Chyzak**[1], **Pierre Lairez**[1], **Bruno Salvy**[2]

Hermite reduction is a classical algorithmic tool in symbolic integration. It is used to decompose a given rational function as a sum of a function with simple poles and the derivative of another rational function. It provides a canonical form modulo derivatives of rational functions. We extend Hermite reduction to arbitrary linear differential operators instead of the pure derivative, and develop efficient algorithms for this reduction. We then apply the generalized Hermite reduction to the computation of linear operators satisfied by definite integrals. The resulting algorithm is a generalization of reduction-based methods for creative telescoping.

Keywords: Hermite reduction, symbolic integration, creative telescoping

[1]INRIA Saclay Île-de-France, France
{alin.bostan,frederic.chyzak,pierre.lairez}@inria.fr

[2]INRIA and LIP – ENS Lyon, France
bruno.salvy@inria.fr

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Solution of non homogenous Ordinary Differential Equations using Parametric Integral Method

Thierry N. Dana-Picard[1], **David G. Zeitoun**[2]

The solution of non homogenous ordinary differential equation (ODE) is an important research subject appearing in numerous engineering fields. When the ODE is associated with boundary conditions (BC), the problem is referred to as a Boundary Value Problem (BVP). Numerical schemes such as finite differences and finite elements have been used for the solution of such problem.

A general homogeneous ODE may be expressed as:

$$\begin{cases} \sum_{n=0}^{n=p} a_n(x)\frac{d^{(n)}y}{dx^n} = 0 \\ a \leq x \leq b \\ (BC) \quad \text{at } x = a \quad \text{and at } x = b \end{cases} \tag{1}$$

This equation may be decomposed into the homogenous part and a non homogenous part, using a MacLaurin expansion of each coefficient $a_n(x)$. For any $n \in \{1, ..., p\}$, we have:

$$a_n(x) = a_n(0) + a_n'(0)x + \frac{x^2}{2}a_n''(0) + ... = \sum_{n=0}^{\infty} \frac{x^n}{n!}a^{(n)}(0) \tag{2}$$

Inserting this last identity into Equation (1) leads to:

$$\begin{cases} L_0(y) = -L(y) \\ a \leq x \leq b \\ (BC) \quad \text{at } x = a \quad \text{and at } x = b \end{cases} \tag{3}$$

where the differential operator L is defined by:

$$L = \sum_{n=0}^{n=p} \left[\sum_{n=1}^{\infty} \frac{x^n}{n!}a^{(n)}(0) \right] \frac{d^{(n)}}{dx^n} \tag{4}$$

The operator L_0 is defined as :

$$L_0 = \sum_{n=0}^{n=p} a_n(0)\frac{d^{(n)}}{dx^n} \tag{5}$$

In this contribution we present a general methodology based on the Adomian decomposition method (ADM) as described in [3]), where the inverse operator L^{-1} is expressed in terms of eigenvectors and eigenvalues expansion. The ADM is a systematic method for solution of either linear or nonlinear operator equations, including ordinary differential equations (ODEs), partial differential equations (PDEs), integral equations, integro-differential equations, etc. The ADM is a powerful technique, which provides efficient algorithms for analytic approximate solutions and numeric simulations for real-world applications in the applied sciences and engineering. It enables to solve both nonlinear initial value problems (IVPs) and boundary value problems (BVPs) (see [5]) without physical restrictive assumptions, such as those required by linearization, perturbation, ad hoc assumptions, and guessing the initial term or a set of basis functions.

Using ADM, we denote a possible solution by $y(x) = \sum_{m=0}^{\infty} y_m(x)$. A general solution of the non homogenous ODE may be found in an iterative way as follows:

- Solve for $y_0(x)$:

$$\begin{cases} L_0(y_0) = 0 \\ a \leq x \leq b \\ (BC) \quad \text{at } x = a \quad \text{and at } x = b \end{cases} \tag{6}$$

- Solve for $y_m(x); m = 1, 2, ...$

$$\begin{cases} L_0(y_m) = -L(y_{m-1}) \\ a \leq x \leq b \\ (BC) \quad \text{at } x = a \quad \text{and at } x = b \end{cases} \tag{7}$$

After solving for $y_0(x)$, the general solution for Equations (7) may be derived using the Green function associated with the operator L_0.

$$\begin{cases} L_0(G(x,\xi)) = \delta(x-\xi) \\ a \leq x \leq b \\ (BC) \quad \text{at } x = a \quad \text{and at } x = b \end{cases}$$

Using Equation (8) and suitable boundary conditions for $G(x,\xi)$, we obtain an iterative solution for $m \geq 1$:

$$y_m(x) = \int_a^b G(x,\xi) L(y_{m-1}(\xi) d\xi \tag{8}$$

In a large class of boundary value problems, the Green function $G(x,\xi)$ may be expressed as an eigenfunction expansion as follows:

$$G(x,\xi) = \sum_{r=1}^{r=q} \frac{\phi_r(x)\phi_r(\xi)}{\lambda_r} \tag{9}$$

where λ_r is the eigenvalue associated with the eigenfunction $\phi_r(x)$ which is the solution of the following ODE:

$$\begin{cases} L_0(\phi_r) = \lambda_r \phi_r \\ a \leq x \leq b \\ (BC) \quad \text{at } x = a \quad \text{and at } x = b \end{cases} \tag{10}$$

So finally the iterative Adomian solution of Equation (7) may be written as:

$$y_m(x) = \sum_{r=1}^{r=q} \frac{\phi_r(x)}{\lambda_r} \int_a^b \phi_r(\xi) L(y_{m-1}(\xi) d\xi \tag{11}$$

In this talk, this last expression will be used to generate different types of iterative algorithms for the solution of the BVP. This iterative algorithm generates an iterative algorithm which can be implemented in a CAS. As examples, we will present solutions of groundwater flow through non homogenous formations using parametric integral solutions. This type of integrals have been already analysed by the authors in [1, 2, 4].

Keywords: parametric integral, non homogenous ODE, Adomian decomposition method

References

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

[2] Th. Dana-Picard and D. G. Zeitoun, Exploration of Parametric Integrals related to a Question of Soil Mechanics, International Journal of Mathematics Education in Science and Technology **48** (4), 617–630 (2017).

[3] G. Adomian, A Review of the Decomposition Method in Applied Mathematics, *Journal of Mathematical Analysis and Applications* **135** (2), 501–544 (1988).

[4] Th. Dana-Picard and D. G. Zeitoun, *A framework for an ICT-Based Study of Parametric Integrals*, Mathematics in Computer Science **11** (3-4), 285–296 (2017).

[5] W.J. Parnell, *Green functions, integral equations and applications*, MATH34032, https://www.scribd.com/document/319286236/greens-notes-pdf (Spring 2013).

[1]Department of Mathematics
Jerusalem College of Technology
Havaad Haleumi St. 21
Jerusalem 9116011
Israel
ndp@jct.ac.il

[2]Mathematics Department
Orot College of Education
Rehovot
Israel
ed.technologie@gmail.com

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Desingularization in the q-Weyl algebra

Christoph Koutschan[1], **Yi Zhang**[2]

The desingularization problem has been primarily studied for linear differential operators with polynomial coefficients. The solutions of such an equation are called *D-finite* functions. It is well known that a singularity at a certain point x_0 of one of the solutions must be reflected by the vanishing (at x_0) of the leading coefficient of the differential equations. However, the converse however is not always true: not every zero of the leading coefficient polynomial induces a singularity of at least one function in the solution space. The purpose of desingularization is to construct another equation, whose solution space contains that of the original equation, and whose leading coefficient vanishes only at the singularities of the previous solutions. Typically, such a desingularized equation will have a higher order, but a lower degree for its leading coefficient. In summary, desingularization provides some information about the solutions of a given differential equation.

The authors of [1, 3] give general algorithms for the Ore case. However, from a theoretical point of view, the story is not yet finished, in the sense that there is no order bound for desingularized operators in the Ore case. We consider the desingularization problem in the first q-Weyl algebra. Our main contribution is to give an order bound for desingularized operators, and thus derive an algorithm for computing desingularized operators in the first q-Weyl algebra. In addition, an algorithm is presented for computing a generating set of the first q-Weyl closure of a given q-difference operator. As an application, we certify that several instances of the colored Jones polynomial from knot theory are Laurent polynomial sequences by computing the corresponding desingularized operator.

Keywords: Desingularization, q-Weyl algebra, Knot Theory

References

[1] S. CHEN, M. KAUERS, AND M. F. SINGER, Desingularization of Ore operators. *Journal of Symbolic Computation*, **74**, 617–626 (2016).

[2] C. KOUTSCHAN AND Y. ZHANG, Desingularization in the q-Weyl algebra. *arXiv 1801.04160*, 1–19 (2018).

[3] Y. ZHANG, Contraction of Ore ideals with applications. In *Proc. of ISSAC'16*, 413–420, ACM, New York, NY, USA, 2016.

[1]Johann Radon Institute for Computational and Applied Mathematics (RICAM)
Austrian Academy of Sciences
Altenbergerstraße 69, A-4040 Linz, Austria
christoph.koutschan@ricam.oeaw.ac.at

[2]Johann Radon Institute for Computational and Applied Mathematics (RICAM)
Austrian Academy of Sciences
Altenbergerstraße 69, A-4040 Linz, Austria
zhangy@amss.ac.cn

S8

Dynamic Geometry and Mathematics Education

Dynamic geometry environments (DGE) have emerged in the last half-century with an ever-increasing impact in mathematics education. DGE enlarges the field of geometric objects subject to formal reasoning, for instance, simultaneous operations with many geometric objects. Today DGE open the possibility of investigating visually and formulating conjectures, comparing objects, discovering or proving rigorously properties over geometric constructions, and Euclidean elementary geometry is required to reason about them.

Along these decades various utilities have been added to these environments, such as the manipulation of algebraic equations of geometric objects or the automated proving and discovering, based on computer algebra algorithms, of elementary geometry statements. Moreover, some intelligent tutoring systems for Euclidean geometry based in DGE have been developed.

The merging of these tools (DGE, automated proving and intelligent tutoring systems) is, thus, a very natural, challenging and promising issue, currently involving logic, symbolic computation, software development, algebraic geometry and mathematics education experts all from over the world.

The Special Session intends to be a forum for:

- presenting the current state of the art concerning the design and implementation of automatic reasoning features on dynamic geometry systems and intelligent tutoring systems;
- fostering a debate concerning the role and use of such features in mathematics education, in general, and their potential impact in proof and proving conception in the classroom, in particular.

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

A new approach to automated study of isoptic curves

Thierry Dana-Picard[1], **Zoltan Kovács**[2]

Let $\mathcal{C}$ be a plane curve. For a given angle θ with $0 \leq \theta \leq 180^\circ$), a θ-*isoptic* of $\mathcal{C}$ is the geometric locus of points in the plane through which pass a pair of tangents with an angle of θ between them. The special case for which $\theta = 90^\circ$ is called an *orthoptic curve*. The orthoptics of conics are well known: the directrix of a parabola, the director circle of an ellipse, and the director circle of a hyperbola (in this case, its existence depends on the eccentricity of the hyperbola).

Orthoptics and θ-isoptics can be studied for other curves, in particular for closed smooth convex curves; see [1]. Isoptics of an astroid are studied in [2] (see Figure 1) and of Fermat curves in [3]. If $\mathcal{C}$ is an astroid, there exist points through which pass 3 tangents to $\mathcal{C}$, and two of them are perpendicular. These works combine geometrical experimentation with a Dynamical Geometry System (DGS) GeoGebra and algebraic computations with a Computer Algebra System (CAS). For them, the curve has been defined by a parametrization. A new approach to these curves is proposed, using

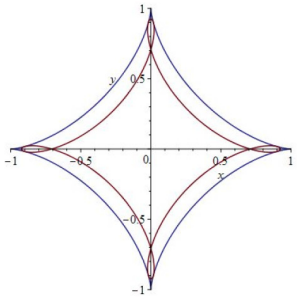


Figure 1: The 45-isoptic of the astroid

the DGS GeoGebra, not only its geometrical part but also its CAS component. The central feature is the connection between the two components of the same software package, enabling automatic switching between different registers of representation. This approach enables to determine the θ-isoptics of various curves, either closed or not. Moreover, the dynamics of the work is essential for the study of the convexity of the θ-isoptic. Students, teachers and researchers can make their own experiments, checking the existence of flexes, changing curves to look for invariant properties, etc.

We demonstrate this approach with GeoGebra applets [4] and [5] for parabolas and other planes curves, either closed or not. Here there is no need to use parametric equations for defining $\mathcal{C}$, and the work is based on implicit equations.

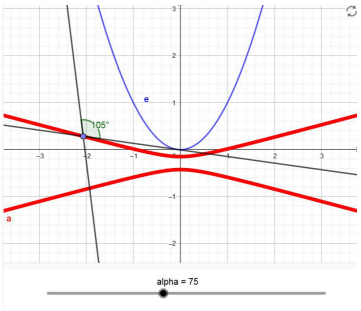


Figure 2: A screenshot of an applet

This automated work allows undergraduates to be acquainted with an advanced topic in Differential Geometry.

Keywords: Plane curves, isoptics, automated proof, dynamical geometry

References

[1] W. Cieslak, A. Miernowski and W. Mozgawa, Isoptics of a closed strictly convex curve, in D. Ferus, U. Pinkall, U. Simon and B. Wegner (edts) *Global Differential Geometry and Global Analysis* LNM 1481, Springer, pp. 28–35 (1990).

[2] Th. Dana-Picard, *An automated study of isoptic curves of an astroid*, Preprint,(2018).

[3] Th. Dana-Picard and A. Naiman, *Isoptics of Fermat Curves*, Preprint, (2018).

[4] Z. Kovacs and Th. Dana-Picard, *Isoptic curves of a parabola*, available: https://www.geogebra.org/m/K5Fyb2dP, (2018).

[5] Z. Kovacs and Th. Dana-Picard, *Computing the orthoptic of a convex quartic*, available: https://www.geogebra.org/m/mfrwfGNc,(2018).

[6] A. Miernowski and W. Mozgawa, On some geometric condition for convexity of isoptics, *Rendinconti Sem. Mat. Universita di Poi. Torino* 55 (2), pp. 93-98 (1997).

[1]Department of Mathematics
Jerusalem College of Technology
Havaad Haleumi St. 21
Jerusalem 9116011
Israel
ndp@jct.ac.il

[2]Mathematics Department
Private University College of Education of the Diocese of Linz
Salesianumweg 3
Linz 4020
Austria
zoltan@geogebra.org

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Discovering properties of bar linkage mechanisms based on partial Latin squares by means of Dynamic Geometry Systems

Raúl M. Falcón[1]

Dynamic Geometry Systems (DGSs) have recently been proposed in mechanical engineering as an alternative to deal with the teach, design, analysis and implementation of mechanisms [1, 6, 7, 8, 9]. Recall that a *mechanism* is any set of rigid bodies connected by *joints* so that force and motion are transmitted among themselves. A *link* within a mechanism is any of its rigid bodies having at least two different joints. A *bar linkage mechanism* is any mechanism in which all its rigid bodies are bars and at least one of them is a link. The study of the relative motion that occurs between each pair of connected bars within one such a mechanism enables its characterization. In this regard, the *degree of freedom of a joint* connecting two bars is defined as the number of independent parameters that are required to determine the relative position of one of the bars with respect to the other one. This has influence on the different *coupler curves* that are generated by the joints within each bar. The study and analysis of such curves enable one to design optimal devices and give rise, therefore, to important applications in Technology and Engineering. Since coupler curves can be described as loci of points satisfying certain geometrical constraints derived from the lengths and connections of bars within a mechanism, DGSs constitute an interesting tool to investigate and characterize them from a visual and dynamical point of view.

In this work, we focus on the use of DGSs to deal with those bar linkage mechanisms such that the distance matrix defined by their joints constitutes a unipotent partial Latin square satisfying certain conditions. Recall that a *partial Latin square* of order n is an $n \times n$ array in which each cell is either empty or contains an element of a finite set of n symbols so that each symbol occurs at most once in each row and in each column. Let $\mathrm{PLS}(n)$ denote the set of partial Latin squares of order n having $[n] := \{0, 1, \ldots, n-1\}$ as set of symbols. The rows and columns of every array in $\mathrm{PLS}(n)$ are supposed to be naturally indexed by the elements of the set $[n]$. Throughout our study, we focus on the subset of partial Latin squares $L = (l_{ij}) \in \mathrm{PLS}(n)$ that are also

i. *reduced*, that is, such that $l_{0i} = i$ and $l_{j0} = j$, for all $i, j \in [n]$ satisfying that the cells $(0, i)$ and $(j, 0)$ in L are non-empty;

ii. *zero-diagonal*, that is, $l_{ii} = 0$, for all $i \in [n]$; and

iii. *symmetric*, that is, $l_{ij} = l_{ji}$, for all $i, j \in [n]$.

To avoid degeneracy and disjoint unions of disconnected mechanisms, we also suppose that

iv. every row and every column of L must contain at least one symbol of the set $[n] \setminus \{0\}$;

v. for each pair $(i, j) \in [n] \times [n]$ such that $l_{ij} \in [n]$, there exists a positive integer $k \in [n]$ such that either $l_{kj} \in [n]$ or $l_{ik} \in [n]$. This involves every bar in the mechanism to be connected to at least one other bar by a joint.

Finally, in order to get linkage mechanisms, the following condition is also required:

vi. If every symbol in $[n] \setminus \{0\}$ appears exactly twice in L, then they cannot be all of them in a same row and column of L.

Let $\mathcal{M}_n$ denote the set of partial Latin squares of order n satisfying Conditions (i)–(vi). This set is preserved by isomorphisms. Recall that two partial Latin squares $L = (l_{ij})$ and $L' = (l'_{ij})$ in $\mathrm{PLS}(n)$ are *isomorphic* if there exists a permutation π on the set $[n]$ such that $\pi(l_{ij}) = l'_{\pi(i)\pi(j)}$, for all $i, j \in [n]$ such that $l_{ij} \in [n]$. To be isomorphic constitutes an equivalence relation among partial Latin squares. The distribution of partial Latin squares into isomorphism classes is known [2, 3, 5], for order $n \leq 6$.

Let $M(L)$ denote the set of bar linkage mechanisms that are associated to a given partial Latin square $L = (l_{ij}) \in \mathcal{M}_n$ as follows:

1. There exists a bar B_{ij} within the mechanism, for each pair $(i, j) \in [n] \times [n]$ such that $i < j$ and $l_{ij} \in [n] \setminus \{0\}$.

2. Two different bars B_{ij} and $B_{i'j'}$ within the mechanism are connected by a joint J_k if and only $\{i, j\} \cap \{i', j'\} = \{k\} \neq \emptyset$. This joint is placed in the corresponding extreme of each bar.

3. Two different bars B_{ij} and $B_{i'j'}$ within the mechanism have the same length if and only if $l_{ij} = l_{i'j'}$.

DGSs constitutes an interesting tool to deal with the study, analysis and characterization of the bar linkage mechanisms in the set $M(L)$. To this end, we consider each symbol $k \in [n] \setminus \{0\}$ to be uniquely associated to a slider s_k so that the length of each bar B_{ij} such that $l_{ij} = k$ is the value given by such a slider s_k (see Figure 1).

In this work, we make use of the mentioned sliders to teach, investigate properties and formulate conjectures about lengths of bars and coupler curves related to those mechanisms associated to partial Latin squares in the set $\mathcal{M}_n$, according to their distribution into isomorphism classes. In this regard, remark the recent study [4] about loci of points whose distance matrix constitutes a partial Latin square satisfying Conditions (i)–(iii). Further, the inclusion on new sliders within each worksheet under consideration enables us to deal with different parameters that characterize our bar

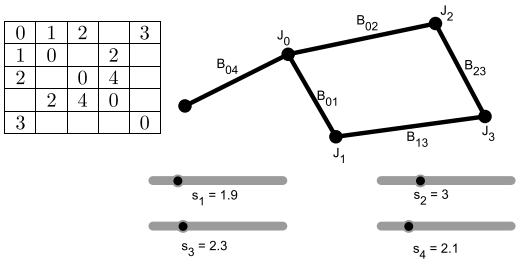


Figure 1: Dynamical study of a bar linkage mechanism based on a partial Latin square.

linkage mechanisms, as the degree of freedom, the transmission ratio, or the mechanical advantage, amongst others. All the constructions that have been developed in this work are available online in the official repository of GEOGEBRA, at the address `https://www.geogebra.org/m/crvJ7CzX`.

Keywords: Linkage systems, dynamic geometry, partial Latin square.

References

[1] B. CORVES, M. HÜSING, M. RIEDEL, Descriptive and Intuitive Mechanism Design and Synthesis Using Geometry-Based Computer-Aided Methods. In *Thirteenth World Congress in Mechanism and Machine Science*. Curran Associates, Inc., Guanajuato, Mexico, 2011.

[2] R. M. FALCÓN, The set of autotopisms of partial Latin squares. *Discrete Math.* **313**, 1150–1161 (2013).

[3] R. M. FALCÓN, Enumeration and classification of self-orthogonal partial Latin rectangles by using the polynomial method. *European J. Combin.* **48**, 215–223 (2015).

[4] R. M. FALCÓN, Two-dimensional loci of points with a partial Latin square within their distance matrix. Submitted, 2018.

[5] R. M. FALCÓN, R. J. STONES, Classifying partial Latin rectangles. *Electron. Notes Discrete Math.* **49**, 765–771 (2015).

[6] Y. HU, N. NELSON-MANEY, P. S. L. ANDERSON, Common evolutionary trends underlie the four-bar linkage systems of sunfish and mantis shrimp. *Evolution* **71**(5), 1397–1405 (2017).

[7] X. IRIARTE, J. AGINAGA, J. ROS, Teaching Mechanism and Machine Theory with GeoGebra. In *New Trends in Educational Activity in the Field of Mechanism and Machine Theory*, J. C. García-Prada, C. Castejón C. (eds.), 211–219, Springer International Publishing, Switzerland, 2014.

[8] S. KURTENBACH, I. PRAUSE, C. WEIGEL, B. CORVES, Comparison of Geometry Software for the Analysis in Mechanism Theory. In *New Trends in Educational Activity in the Field of Mechanism and Machine Theory*, J. C. García-Prada, C. Castejón (eds.), 193–201, Springer International Publishing, Switzerland, 2014.

[9] I. PRAUSE, J. C. FAUROUX, M. HÜSING, B. CORVES, Using Geometry Sketchers and CAD Tools for Mechanism Synthesis. In *Proceedings of IFToMM 2015, The 14th World Congress in Mechanism and Machine Science*, paper OS3-032, 11 pp., International Federation for the Theory of Mechanisms and Machines, Taiwan, 2015.

[1]School of Building Engineering.
Department of Applied Mathematics I.
University of Seville.
Avda. Reina Mercedes 4A. 41012 - Seville (Spain).
rafalgan@us.es

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Exploration of dual curves using dynamic geometry and computer algebra system

Roman Hašek[1]

This submission deals with the use of the dynamic mathematics software GeoGebra to determine the dual curve to the given curve and inspect its properties. The combination of dynamic geometry tools with computer algebra functions allows a user to take both geometric and algebraic perspectives on this issue. The dual curve to an algebraic curve is a curve born from the duality between points and lines in the projective plane. Writing the equation of a curve laying in this plane in homogeneous coordinates $[x_0, x_1, x_2]$ its tangents can be taken as points in the dual plane written in the coordinates $[y_0, y_1, y_2]$. Then the locus of these points is the dual curve to the given curve, [2].

We will show both the geometric model of the dual curve and the algebraic derivation of its equation in the talk. The geometric approach to display the dual curve shape is based on the polar reciprocity which is realized through the inversion in a circle here, [3, 4], see Fig. 1.

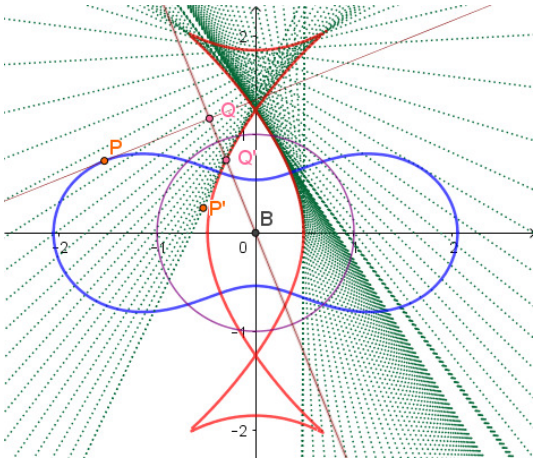


Figure 1: Dual curve to the Cassini oval as an envelope of lines dual to the points of the oval

The algebraic derivation of the dual curve equation is based on the idea that the related polynomial in indeterminates y_0, y_1, y_2 is a component of the Gröbner basis of the ideal of polynomials describing the aforesaid act of transition from a tangent

line of the curve in a projective space to the point in its dual space, [5]. For example, considering the astroid with the Cartesian equation

$$27x^2y^2 + (x^2 + y^2 - 1)^3 = 0, \tag{1}$$

written in homogeneous coordinates $[x_0, x_1, x_2]$ as

$$h = x_0^6+x_1^6-x_2^6+3x_0^2x_1^4+3x_0^2x_2^4+3x_0^4x_1^2-3x_0^4x_2^2+3x_1^2x_2^4-3x_1^4x_2^2+21x_0^2x_1^2x_2^2 = 0, \tag{2}$$

the polynomial defining its dual is such a member of the Gröbner basis of the ideal of polynomials in indeterminates $x_0, x_1, x_2, y_0, y_1, y_2$

$$I = \langle y_0 - h'_{x_0}, y_1 - h'_{x_1}, y_2 - h'_{x_2}, h\rangle \tag{3}$$

that contains only indeterminates y_0, y_1, y_2. Its existence follows from the Elimination theorem, [1]. To derive the equation in GeoGebra we use the `Eliminate` command and, after transformation into the Cartesian equation

$$x^2y^2 - x^2 - y^2 = 0, \tag{4}$$

we can display the dual curve as shown in Fig. 2.

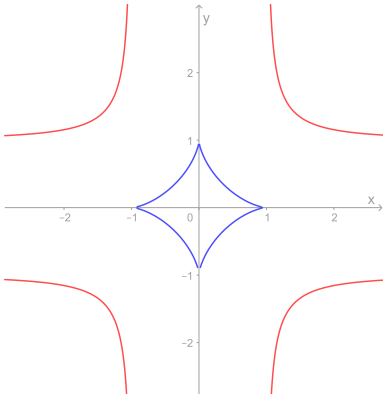


Figure 2: Dual curve (red) to the astroid (blue)

Apart from modeling the dual curve and the derivation of its equation we will also focus on the educational potential of this topic in the talk. The history of the notion of the dual curve is inter alia associated with the story of "the duality paradox" [3], which is worth mentioning when the concept of duality of projective space is taught. Moreover, the relation between a curve and its dual reveals concrete examples of how the duality works, [4]. See for example the correspondence between points and lines belonging to the dual curves in Figure 3, namely the correspondence between bitangents of the oval and nodes of its dual curve or the correspondence between inflexion points of the former and the cusps, more precisely tangents in them, of the latter. The utilization of dynamic geometry to explore these situations will also be presented through several particular examples.

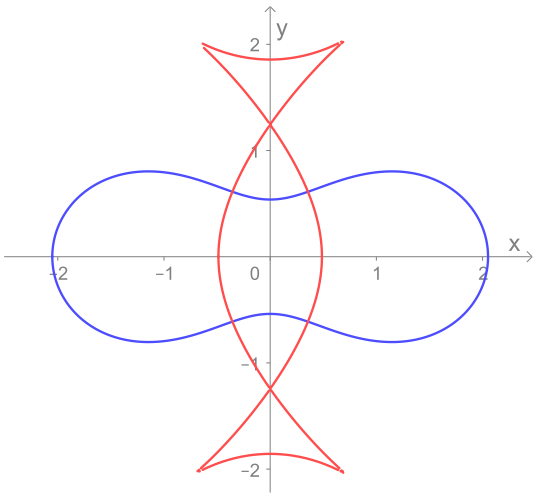


Figure 3: The Cassini oval (blue) and its dual curve (red)

Keywords: Computer algebra, dual curve, dynamic geometry, Gröbner basis

References

[1] D. A. Cox; J. B. Little; D. O'Shea, *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. 3rd ed. Springer, New York, 2007.

[2] C. G. Gibson, *Elementary geometry of algebraic curves: an undergraduate introduction*. Cambridge University Press, New York, 1998.

[3] J. Gray, *Worlds out of nothing: a course in the history of geometry in the 19th century*. [2nd ed.]. Springer, Springer undergraduate mathematics series, London, 2011.

[4] M. Monks, *Duality of Plane Curves*, 2011. Available at `https://www.math.ucdavis.edu/~mgillespie/papers/DualityV3.pdf`. Accessed 29 March 2018.

[5] H. Pottmann; J. Wallner, *Computational line geometry*. 1. Springer, New York, 2001.

[1]Department of Mathematics
University of South Bohemia in České Budějovice
Faculty of Education
Jeronýmova 10
371 15 České Budějovice
Czech Republic
hasek@pf.jcu.cz

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Issues and challenges about instrumental proof

Philippe R. Richard[1], **Fabienne Venant**[2], **Michel Gagnon**[3]

The notion of instrumental proof is relatively new. If the term is little used in didactic literature, its natural association with technologies, old and new, seems self-evident.

On the epistemological side, the discovery of Archimedes's palimpsest recently allowed us to better understand how the weighing method was a kind of mechanical proof, which suggests to the point that the association between proof and artifacts/tools is rather old. Similarly, computer proofs such as those of the four-colour theorem –first shown in 1976 by Kenneth Appel and Wolfgang Haken, then formally addressed in 2005 using Coq software by Georges Gonthier and Benjamin Werner– offer proofs where they are algorithms that base the decision or the verification of all cases, reflecting an unavoidable reality of contemporary mathematical work. Whether they are physical or logical, the use of tools in a validation situation certainly renews the usual idea that we have between the concepts of proof, modelling and representation of knowledge.

On the didactic side, there seems to be a constant struggle with paradoxes. The student is asked to prove propositions, but he or she now has an automated reasoning tool. It requires him or her to work with meaningful knowledge and to transform it, but by working more and more at the interface of computer tools that manage both a part of the representation and treatment, and often even experimenting on mathematical objects (e.g. dynamic figures) as a physicist does with objects of his own domain. And all this, without the teacher can refer to mathematics that could be described as technological, since he was initiated to a deductive science that has developed traditionally in writing.

It is then by extending ideas that we have already exposed in our work, including the recent paper [3], *The Concept of Proof in the Light of Mathematical Work*, and resuming conclusions of our current research projects (design of the tutorial system QED-Tutrix in high school geometry [1], the use of the Automated Reasoning Tools (ART) [2] in teacher training) that we approach the question of instrumental proofs. With this attitude, the subject-milieu interaction is a unit of epistemic necessity, the subject can be both a reader, to consider traditional proofs, and the user of software or a mathematical machine. The notions of reasoning in action and reasoning that unfold differently than with the discourse will be treated, as well as the theory of mathematical working spaces in which the question of the coordination of discursive, semiotic and instrumental geneses arise between an epistemological and a cognitive plan.

Keywords: Instrumental proof, mathematical working space, instrumented reasoning, algorithmic, physics

References

[1] L. FONT, P. R. RICHARD AND M. GAGNON, Improving QED-Tutrix by Automating the generation of Proofs. In: Pedro Quaresma and Walther Neuper (Eds.): *Proceedings 6th International Workshop on Theorem proving components for Educational software, (ThEdu'17), Electronic Proceedings in Theoretical Computer Science*, **267**, 38-58, (2018).

[2] Z. KOVÁCS, P.R. RICHARD, T. RECIO AND M.P. VÉLEZ, GeoGebra Automated Reasoning Tools: A tutorial with examples. In: G. Aldon, G. and J. Trgalova (Eds.): *Proceedings of the 13th International Conference on Technology in Mathematics Teaching*. https://hal.archives-ouvertes.fr/hal-01632970.

[3] P.R. RICHARD, A.M. OLLER AND V. MEAVILLA, The Concept of Proof in the Light of Mathematical Work *ZDM - The International Journal on Mathematics Education,* **48** (6), 843-859, (2016). (DOI: 10.1007/s11858-016-0805-9)

[1]Université de Montréal
philippe.r.richard@umontreal.ca

[2]Université du Québec à Montréal
venant.fabienne@uqam.ca

[3]École Polytechnique de Montréal
michel.gagnon@polymtl.ca

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Programming in KeTCindy with Combined Use of Cinderella and Maxima

S. Takato[1], **S. Yamashita**[2] **J.A. Vallejo**[1]

Printed materials are often distributed to the classes at the college level. For such materials, line drawing type figures are more suitable. KeTCindy, a macro package of CindyScript which is a programming language implemented in Cinderella, supports line drawing of 3D figures. To produce these 3D figures with KeTCindy, it is fundamentally important to find intersections of projection curves. The combined use of KeTCindy, Cinderella, and Maxima is an effective tool to develop such programs.

Keywords: KeTCindy, Cinderella, Maxima

Mathematics teachers at the college level often distribute printed materials to their alumni. For such materials, figures presented as line drawings are better suited, because students can write their own remarks over them on the paper. KeTCindy, a macro package of CindyScript (which is a programming language implemented in Cinderella), can produce fine figures for LaTeX. Furthermore, KeTCindy supports line drawing of 3D figures as explained below.

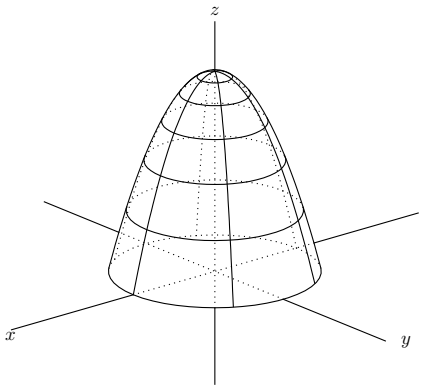


Fig.0

To produce these 3D figures, KeTCindy follows the following steps:

1. To find silhouette lines of the surface, in the figure above those are given by $x = u\cos v,\ y = u\sin v,\ z = 4 - u^2$. Data are obtained from an implicit function of the form

$$J(u,v) = \frac{dX}{du}\frac{dY}{dv} - \frac{dX}{dv}\frac{dY}{du} = 0\,,$$

where $(X, Y) = \mathrm{Proj}(x, y, z)$ is the map to the plane of projection.

2. To find the intersections of silhouette lines and a projection curve.

3. To divide the curve by these intersects, and to decide whether each separation is hidden by the surface or not.

Of the above, the second item is of fundamental importance, but it represents a difficult task in the case of contacting curves because curves are numerically polygonal lines. The following figures demonstrate this setting: The right panel shows an enlarged figure at a contact point presented on the left.

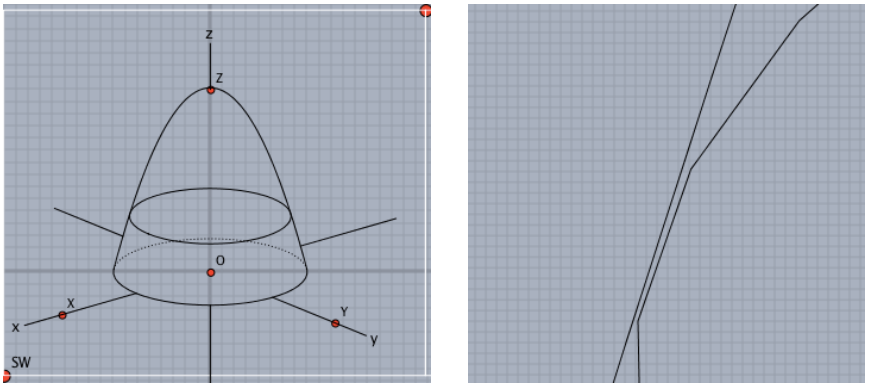


Fig.1

To refine the calculation of item 2, we have adopted an interpolatory scheme using Bézier curves near the contact point. Then we use a formula developed by Oshima[1] to decide the control points.

The left in the following is a further enlarged figure. The right shows Bézier curves in red color.

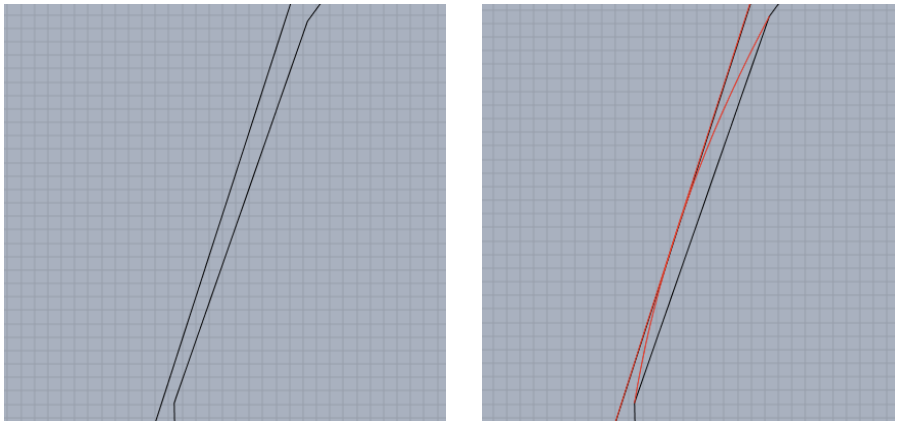


Fig.2

In this setting, the intersect is represented by a cluster of points. One of them is

$$\mathrm{P} = [-1.65827, 1.20578]. \tag{1}$$

KETCindy can also call Maxima from Cinderella and return a result back to Cinderella. For example, the intersect for Figure 2 is calculable using the following script in CindyScript. The result is:

$$\mathrm{P} = [-1.656701299244927, 1.210755779027779], \tag{2}$$

confirming that (1) is a very good approximation to the contact point.

```
cmdL=[
 "ph:50/180*%pi",[],
 "th:70/180*%pi",[],
 "sp:float(sin(ph))",[],
 "cp:float(cos(ph))",[],
 "st:float(sin(th))",[],
 "ct:float(cos(th))",[],
 "proj(x,y,z):=[-x*sp+y*cp,-x*cp*ct-y*sp*ct+z*st]",[],
 "P:proj(u*cos(v),u*sin(v),4-u^2)",[],
 "J:diff(P[1],u)*diff(P[2],v)-diff(P[1],v)*diff(P[2],u)",[],
 "u0:5/3",[],
 "J:ev(J,[u=u0])",[],
 "J:expand(J)",[],
 "eq1:ev(J,[cos(v)=c,sin(v)=s])",[],
 "eq1:ev(eq1,[c^2=1-s^2])",[],
 "eq:[eq1=0,c^2+s^2=1]",[],
 "ans:solve(eq,[c,s])",[],
 "ans:float(ans)",[],
 "Q:proj(u0*c,u0*s,4-u0^2)",[],
 "A:ev(Q,ans[1])",[],
 "B:ev(Q,ans[2])",[],
 "A::B",[]
];
CalcbyM("ans",cmdL);
println(ans);
```

```
generate spacecurve sc3d1
      CalcbyM succeeded ans (0.01 sec)
[[1.656701299244927,1.210755779027779],[-1.656701299244927,1.210755779027779]]
```

Fig.3

As a conclusion, we could say that the combined use of KETCindy, Cinderella, and Maxima is an effective tool to develop programs for surface drawing.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number 16K01152.

References

[1] Oshima, T., Drawing curves, Symposium MEIS2015: Mathematical Progress in Expressive Image Synthesis, MI Lecture Notes 2015 **64**, 117–120, Kyushu University, 2015

[2] Takato S., What is and how to Use KeTCindy – Linkage Between Dynamic Geometry Software and Collaborative Use of KetCindy and Free Computer Algebra Systems and LaTeX Graphics Capabilities –, Mathematical Software –ICMS 2016, LNCS **9725**, 371–379, Springer, 2016.

[1]Department of Science,
Toho University
2-2-1, Miyama, Funabashi, 274-8510, Japan
takato@phar.toho-u.ac.jp

[2]Department of Natural Science,
National Institute of Technology, Kisarazu College
2-11-1, Kiyomidai-Higashi, Kisarazu, 292-0041, Japan
yamasita@kisarazu.ac.jp

[3]Faculty of Science,
Universidad Autónoma de San Luis Potos
Av. Salvador Nava s/n 78290, San Luis Potosí, MEXICO
jvallejo@fciencias.uaslp.mx

S9

Computer Algebra in Coding Theory and Cryptography

This session aims to bring together from all areas related to computer algebra (both theoretical and algorithmic) applied to Coding Theory and Cryptography.

Since much of the work related to these topic is recent or is still ongoing, this session will provide a stimulating forum where experts will be able to not only report their recent results, but also to propose new lines of research and discuss open questions.

It will also give us the opportunity to present the interest and the potential applications of these topics to the rest of the scientific community

Expected topics of presentations include (but are not limited to):

- Computer Algebra and Coding Theory
  Codes and applications. Combinatorial structures. Algebraic-geormetric codes. Network coding. Quantum codes. Group codes. . .
- Computer Algebra in Cryptography
  Algebraic Cryptanalysis. Post-quantum cryptography. (Code, Lattice and Hash)–based PKC. Multivariate PKC. . .
- simulation of quantum computation
- Synergies between Computer Algebra, Coding Theory and Cryptography.

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

The enumeration of Hermitian self-dual cyclic codes over finite chain rings

Arunwan Boripan[1], **Somphong Jitman**[2], **and Patanee Udomkavanich**[3]

Let $\mathbb{F}_{q^2}$ be a finite field of order q^2 and let $R := \mathbb{F}_{q^2}[u]/\langle u^t \rangle$ be a finite chain ring, where $t \geq 2$ is an integer. Cyclic codes over R have been of interest due to their rich algebraic structures and wide applications. Here, the characterization and enumeration of Hermitian self-dual cyclic codes of length n over R have been given based on self-conjugate-reciprocal irreducible monic(SCRIM) factors of $x^n - 1$ over $\mathbb{F}_{q^2}$. Subsequently, the number of SCRIM factors of $x^n - 1$ over $\mathbb{F}_{q^2}$ has been investigated. Finally, some computational results obtained from computer algebra MAGMA have been discussed.

Keywords: Cyclic codes, Hermitian self-dual cyclic code, Finite chain ring

References

[1] A. BORIPAN; S. JITMAN; P. UDOMKAVANICH, Self-Conjugate-Reciprocal Irreducible Monic Polynomials over Finite Fields. In *Proccedings of the 20th Annual Meeting in Mathematics 2015*, Department of Mathematics, Faculty of Sceince, Silapakorn University, 34–43. Nakorn Pathom, 2015.

[2] B. CHEN; S. LING; G. ZHANG, Enumeration formulas for self-dual cyclic codes. *Finite Fields and Their Applications* **42**, 1–22 (2016).

[1]Department of Mathematics and Computer Science, Faculty of Science
Chulalongkorn University
Bangkok 10330, Thailand
boripan-arunwan@hotmail.com

[2]Department of Mathematics, Faculty of Science
Silapakorn University
Nakhon Pathom 73000, Thailand
sjitman@gmail.com

[3]Department of Mathematics and Computer Science, Faculty of Science
Chulalongkorn University
Bangkok 10330, Thailand
pattanee.u@chula.ac.th

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Binary Isodual Codes Having an Automorphism of Odd Prime Order*

Stefka Bouyuklieva[1], **Radka Russeva**[2], **Emine Karatash**[2]

The purpose of this talk is to describe the structure and properties of the binary isodual codes having automorphisms of odd prime order and to present a method for their construction. If a code C is equivalent to its orthogonal complement $C^{\perp}$, then it is termed *isodual*, and if $C = C^{\perp}$, C is a *self-dual* code. Recently, there has been growing interest in the isodual codes, and the authors use different methods for their construction (see for example [5]).

A linear code C is formally self-dual if C and its dual $C^{\perp}$ have the same weight enumerator. While self-dual codes contain only even weight vectors, formally self-dual codes may contain odd weight codewords as well. Many authors consider only even formally self-dual codes because their weight enumerators are combinations of Gleason polynomials. The class of isodual codes is between the self-dual and formally self-dual (fsd) codes. Since all isodual codes are also formally self-dual, they possess all the properties of the fsd codes.

The minimum weight d of a formally self-dual even code of length n is bounded by $d \leq 2[n/8] + 2$. An fsd even code meeting this upper bound is called extremal. Self-dual codes meeting this bound exist only for lengths $n = 2$, 4, 6, 8, 12, 14, 22 and 24 [3]. Extremal formally self-dual even codes which are not self-dual exist only for lengths 6, 10, 12, 14, 18, 20, 22, 28 and 30, and all these codes are classified [2]. For some lengths, there are odd fsd codes with higher minimum weight than the even ones. For example, the unique linear $[16, 8, 5]$ code has dual distance 5 and therefore it is formally self-dual, but the highest possible minimum weight of an even code of the same length is 4 (see [6]). The smallest length for which a fsd code is not isodual is 14, and there are 28 such codes amongst 6 weight enumerators. The even fsd $[30, 15, 8]$ codes are classified (see [2]) but it is still not known whether odd fsd codes with these parameters exist.

In the eighties of the last century, Huffman and Yorgov proposed a method for constructing and classifying binary self-dual codes with an automorphism of odd prime order (see [4, 7]). This method can be modified and applied to other linear codes. The closest class is the class of binary isodual codes, and therefore we study the structure of those isodual codes that have an automorphism of odd prime order. Let C be a binary linear code of length n and σ be an automorphism of C of odd prime order p with c independent p-cycles. Without loss of generality we can assume

*This research is supported by Bulgarian Science Fund under Contract DN-02-2/13.12.2016 and by Shumen University, Project RD-08-111/ 05.02.2018

that $\sigma = \Omega_1 \dots \Omega_c \Omega_{c+1} \dots \Omega_{c+f}$, where $\Omega_i = ((i-1)p+1, \dots, ip), i = 1, \dots, c$, are the cycles of length p, and $\Omega_{c+i} = (cp+i), i = 1, \dots, f$, are the fixed points. Obviously, $cp + f = n$.

Let $F_\sigma(C) = \{v \in C : v\sigma = v\}$ and $E_\sigma(C)$=$\{v \in C : wt(v|\Omega_i) \equiv 0 \pmod 2, i = 1, \dots, c+f\}$, where $v|\Omega_i$ is the restriction of v on Ω_i. Then the code C is a direct sum of the subcodes $F_\sigma(C)$ (fixed subcode) and $E_\sigma(C)$ (even subcode).

Consider first the fixed subcode. Clearly, $v \in F_\sigma(C)$ if and only if $v \in C$ and v is constant on each cycle. Let $\pi : F_\sigma(C) \to F_2^{c+f}$ be the projection map, so if $v \in F_\sigma(C)$, $(v\pi)_i = v_j$ for some $j \in \Omega_i, i = 1, 2, \dots, c+f$. Denote by C_π the code $\pi(F_\sigma(C))$.

For $v \in E_\sigma(C)$ and $1 \le i \le c$, we identify $v|\Omega_i = (v_0, v_1, \cdots, v_{p-1})$ with the polynomial $v_0 + v_1 x + \cdots + v_{p-1}x^{p-1}$ from $\mathcal{P}$, where $\mathcal{P}$ is the set of even-weight polynomials in $\mathbb{F}_2[x]/(x^p - 1)$. Thus we obtain the map $\phi : E_\sigma(C) \to P^c$. Denote $\phi(E_\sigma(C))$ by C_ϕ. Obviously, C_ϕ is a $\mathcal{P}$-module, and if $\mathcal{P}$ is a field then C_ϕ is a linear code. On $\mathcal{P}^c$, we use the Hermitian inner product:

$$\langle u, v \rangle = \sum_{j=1}^{c} u_j \overline{v_j}, \tag{1}$$

where $\overline{v_j} = v_j(x^{-1}) = v_j(x^{p-1})$, $u = (u_1, \dots, u_c)$, $v = (v_1, v_2, \dots, v_c)$.

For the equivalence we use the following theorem

Theorem 1: *The following transformations preserve the decomposition and send the code C to an equivalent one:*

a) the substitution $x \to x^t$ in C_φ, where t is an integer, $1 \le t \le p-1$;

b) multiplication of the jth coordinate of C_φ by x^{t_j} where t_j is an integer, $0 \le t_j \le p-1$, $j = 1, 2, \dots, c$;

c) permutation of the first c cycles of C;

d) permutation of the last f coordinates of C.

If $\sigma \in Aut(C)$, $\sigma \in Aut(C')$, and p^2 does not divide the orders of both groups, then the codes C and C' are equivalent if and only if C' can be obtained from C by applying a sequence of the given transformations.

The proof is similar to the proof of Theorem 3 in [7].

Now let C be a binary isodual code, so $C \cong C^\perp$. Since $Aut(C) = Aut(C^\perp)$, the permutation σ is an automorphism of $C^\perp$, too. Hence $C^\perp = F_\sigma(C^\perp) \oplus E_\sigma(C^\perp)$. Let $C'_\pi = \pi(F_\sigma(C^\perp))$, and $C'_\phi = \phi(E_\sigma(C^\perp)^*)$.

If 2 is a multiplicative root modulo p then $\mathcal{P}$ is a field with 2^{p-1} elements and C_ϕ is a linear code over this field. Therefore here we consider only such primes p. We say that two codes over $\mathcal{P}$ are equivalent if one of them can be obtain from the other one after a sequence of transformations of types a), b) and c) from Theorem 1. Using this theorem, we obtain the following results.

Theorem 2: *The binary codes C_π and C'_π are equivalent. The same is true for the codes C_ϕ and C'_ϕ over the field $\mathcal{P}$.*

Theorem 3: *Let C be a binary linear $[2k, k, d]$ code having an automorphism σ of odd prime order p. If 2 is a multiplicative root modulo p and p^2 does not divide the order of Aut(C) then C is an isodual code if and only if the codes C_π and C_ϕ are isodual.*

As an application of the presented structure we focus on the isodual $[30, 15, \geq 7]$ codes with an automorphism of order 5 with 6 independent 5-cycles. If C is such a code, then C is a direct sum of a $[30, 3, \geq 10]$ fixed subcode projected in a binary $[6, 3, \geq 2]$ isodual code C_π, and a $[30, 12, \geq 8]$ even code $E_\sigma(C)$. There exist exactly six binary isodual codes of length 6, one of them has minimum distance 3, and the other five codes have minimum distance 2, including the only self-dual $[6, 3, 2]$ code. The only isodual $[6, 3, 3]$ code has weight enumerator $1 + 4y^3 + 3y^4$ [6].

The image of the even subcode under the map ϕ is a $[6, 3, d_\phi]$ linear code over the field $\mathcal{P} \cong GF(16)$. For the field we have $\mathcal{P}^* = \{\alpha^i \delta^j,\ i = 0, 1, \ldots, 4,\ j = 0, 1, 2\}$, where $e = x + x^2 + x^3 + x^4$ is the identity element, $\alpha = xe$ is an element of order 5, and $\delta = x + x^4$ is of order 3.

First, we constructed all $[6, 3, d_\phi]$ linear codes over $\mathcal{P}$ such that $d(\phi^{-1}(M)) \geq 8$. There are 61 $[6, 3, 3]$ and 326 $[6, 3, 4]$ inequivalent codes with the needed properties. Then we combined these codes with all codes $\pi^{-1}(C')$ where C' is equivalent to any of the isodual $[6, 3, \geq 2]$ binary codes. After that we check all these binary isodual codes of length 30 for minimum weight and also for equivalence, using the program Q-EXTENSION [1]. In this way we obtained exactly 642 binary isodual $[30, 15, \geq 7]$ inequivalent codes having an automorphism of order 5 with 6 independent 5-cycles. Only 13 of these codes have minimum weight 8. All constructed $[30, 15, 8]$ codes have the same weight enumerator $1 + 450y^8 + \cdots + y^{30}$ and so they are even isodual codes.

Keywords: linear codes, isodual codes, automorphisms

References

[1] I. BOUYUKLIEV, What is Q-EXTENSION? *Serdica J. Computing* **1**, 115–130, (2007).

[2] S. BOUYUKLIEVA; I. BOUYUKLIEV, Classification of the extremal formally self-dual even codes of length 30. *Adv. in Mathematics of Communications* **4**, 433–439, (2010).

[3] J.H. CONWAY; N.J.A. SLOANE, A new upper bound on the minimal distance of self-dual codes. *IEEE Trans. Inform. Theory* **36** 1319–1333, (1991).

[4] W.C. HUFFMAN, Automorphisms of codes with application to extremal doubly-even codes of lenght 48. *IEEE Trans. Inform. Theory* **28**, 511–521 (1982).

[5] H.J. KIM; Y. LEE, Construction of isodual codes over $GF(q)$. *Finite Fields and Their Applications* **45**, 372–385, (2017).

[6] SUNGHYU HAN; HEISOOK LEE; YOONJIN LEE, Binary formally self-dual odd codes. *Designs, Codes and Cryptography* **61**, 141–150 (2011).

[7] V. YORGOV, A method for constructing inequivalent self-dual codes with applications to length 56. *IEEE Trans. Inform. Theory* **33**, 77–82 (1987).

[1]Faculty of Mathematics and Informatics
"St. Cyril and St. Methodius" University of Veliko Tarnovo
Bulgaria
stefka@ts.uni-vt.bg

[2]Faculty of Mathematics and Informatics
Shumen University
Bulgaria
russeva@fmi.shu-bg.net, e.karatash@abv.bg

Theorem [theorem]Lemma [theorem]Proposition [theorem]Example
Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Multiplying Dimension in Abelian Codes

José Joaquín Bernal[1], **Diana H. Bueno-Carreño**[2] , **Juan Jacobo Simón**[1]

In [1], we improve the notion and computation of the apparent distance for abelian codes given in [4] and [7] by means of the q-orbit structure of defining sets of abelian codes. These results allows us to design, based on a suitable election of q-orbits, abelian codes having nice bounds and parameters. In this note, we apply those techniques to construct bivariate BCH codes from cyclic codes, in such a way that we preserve apparent distance but multiplying their dimension; in particular, this drives us to multiply Reed-Solomon codes to abelian codes. As it happens with others families of abelian codes, there are alternative constructions to get this one (see, for example [6]); however, we think that this point of view allows us to determine many structural properties, parameters and even true minimum distance, in a better way.

We denote $I = \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$ and for $i = 1, 2$, we denote by U_{r_i} the set of all r_i-th primitive roots of unity and define $U = U_{r_1} \times U_{r_2}$. It is a known fact that, for a fixed $\hat{\alpha} = (\alpha, \beta) \in U$, any abelian code C is determined by its defining set, with respect to $\hat{\alpha}$, which is defined as

$$\mathcal{D}_{\hat{\alpha}}(C) = \left\{ (a, b) \in I \ : \ c(\alpha^a, \beta^b) = 0, \ \forall c \in C \right\}.$$

In [1], we introduced the notion of strong apparent distance of polynomials and hypermatrices and we applied it to define and study a notion of multivariate BCH bound and BCH abelian codes. As it was pointed out in the mentioned paper, the notion of strong apparent distance was based in the ideas and results in [4] and [7].

We use those results and techniques to prove the following results, among others.

Theorem 5. *Let n and r be positive integers such that $\gcd(q, nr) = 1$. Let C be a nonzero cyclic code in $\mathbb{F}_q(r) = \mathbb{F}_q[y]/(y^r - 1)$ with $sd^*(C) = \delta > 1$ and $\hat{\alpha} = (\alpha_1, \alpha_2) \in U_n \times \mathcal{R}(C)$. Then, the abelian code C_n in $\mathbb{F}_q(n, r) = \mathbb{F}_q[x, y]/(x^n - 1, y^r - 1)$ with defining set $\mathcal{D}_{\hat{\alpha}}(C_n) = \mathbb{Z}_n \times \mathcal{D}_{\alpha_2}(C)$ verifies that $sd^*(C_n) = \delta$ and $\dim_{\mathbb{F}_q}(C_n) = n \dim_{\mathbb{F}_q}(C)$.*

Proposition 6. Let n and r be positive integers with $\gcd(q, nr) = 1$ and let C be a nonzero cyclic code in $\mathbb{F}_q(r)$ such that $sd^*(C) = d(C)$. Then there exists $\hat{\alpha} = (\alpha_1, \alpha_2) \in U_n \times \mathcal{R}(C)$ such that the abelian code C_n in $\mathbb{F}_q(n, r)$ with defining set $\mathcal{D}_{\hat{\alpha}}(C_n) = \mathbb{Z}_n \times \mathcal{D}_{\alpha_2}(C)$ verifies the equality $d(C_n) = d(C)$.

BCH multivariate codes have also been defined in [1, Definition 33]. Following this definition we prove the following result.

Proposition 7. Let $\alpha \in U_r$ and let $R = B_q(\alpha, \delta, b)$ be a Reed-Solomon code. Then, for each positive integer n and any $\alpha' \in U_n$, there exists a multivariate BCH code, $C = B_q((\alpha', \alpha), \{2\}, \{\delta\}, \{b\})$, such that $\dim(C) = (r - \delta + 1)\, n = n \cdot \dim(R)$ and $d(C) = sd^*_{\hat{\alpha}}(C) = \delta$.

Some examples and applications will be presented.

Keywords: Abelian codes, Multiplying dimension, Cyclic codes, Reed-Solomon codes

References

[1] J.J. Bernal, D.H. Bueno-Carreño, J.J. Simón, Apparent distance and a notion of BCH multivariate codes. *IEEE Trans. Inform. Theory*, **62**(2), 655-668, 2016.

[2] J.J. Bernal, D.H. Bueno-Carreño, J.J. Simón, Cyclic and BCH Codes whose Minimum Distance Equals their Maximum BCH bound, Adv Math Comm, 10 (2016), 459-474.

[3] J. J. Bernal, M. Guerreiro, J. J. Simón, From ds-bounds for cyclic codes to true minimum distance for abelian codes. Submitted.

[4] P. Camion, *Abelian Codes*, MRC Tech. Sum. Rep. # 1059, University of Wisconsin, 1971.

[5] H. Imai, A theory of two-dimensional cyclic codes. *Information and Control* **34**(1) (1977) 1-21.

[6] J. M. Jensen, The concatenated structure of cyclic and abelian codes, *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 788-793, 1985.

[7] R. Evans Sabin, On Minimum Distance Bounds for Abelian Codes, *Applicable Algebra in Engineering Communication and Computing*, Springer-Verlag, 1992.

[1]Departamento de Matemáticas
Universidad de Murcia, 30100 Murcia, Spain.
{josejoaquin.bernal, jsimon}@um.es

[2]Departamento de Ciencias Naturales y Matemáticas
Pontificia Universidad Javeriana, Cali, Colombia
dhbueno@javerianacali.edu.co

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

On the skew cyclic codes and the reversibility problem for DNA 4-bases

Yasemin CENGELLENMIS[1], **Abdullah DERTLI**[2]

The skew cyclic codes over the finite ring $R = F_4 + uF_4 + vF_4 + uvF_4$, where $u^2 = u, v^2 = v, uv = vu$ are introduced, by defining a non trivial automorphism over R. DNA 4-bases are matched with the elements 256 of the finite ring R. With the method as in [3], the reversible DNA codes are obtained. Moreover, the Gray images of the skew cyclic codes over the finite ring R are determined.

Keywords: Reversible code, DNA cyclic code

References

[1] BAYRAM A.; OZTAS E.; SIAP I., *Codes over $F_4 + vF_4$ and some DNA applications*. Designs, Codes and Cryptography,80,379-393, DOI: 10.1007/s10623-015-0100-8, (2016).

[2] DERTLI A. ; CENGELLENMIS Y, *On cyclic DNA codes over the finite rings $Z_4 + wZ_4$ and $Z_4 + wZ_4 + vZ_4 + wvZ_4$*, *Biomath* , **6**, 1-11 ,(2017).

[3] GURSOY F.; OZTAS S. E.; SIAP I, *Reversible DNA codes over $F_{16} + uF_{16} + vF_{16} + uvF_{16}$*, arXiv:1703.10189v1, (2017).

[1]Department of Mathematics
Trakya University
Balkan Campus, Edirne ,Turkey
ycengellenmis@gmail.com

[2]Department of Mathematics
Ondokuz Mayıs University
Samsun, Turkey
abdullah.dertli@gmail.com

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Quantum codes from constacyclic codes over the finite ring $F_p + uF_p + vF_p$

Abdullah Dertli[1], **Yasemin Cengellenmis**[2]

In this paper, the quantum codes over F_p from constacyclic codes over the finite ring $F_p + uF_p + vF_p$, where $u^2 = u, v^2 = v, uv = vu = 0$, p is an odd prime are studied. A constacyclic codes over the finite ring $F_p + uF_p + vF_p$ is decomposed into three codes over F_p in order to determine the parameters of the corresponding quantum codes. Finally, we have constructed some examples of quantum error-correcting codes.

Keywords: Quantum code, Constacyclic code, Finite ring

References

[1] DERTLI A., CENGELLENMIS Y., EREN S., On quantum codes obtained from cyclic codes over A_2. *International journal of quantum information* **13**(03), 1550031 (2015).

[2] DERTLI A., CENGELLENMIS Y., EREN S., Some results on the linear codes over the finite ring $F_2+v_1F_2+...+v_rF_2$. *International journal of quantum information* **14**(01), 1650012 (2016).

[3] GAO J., WANG Y., u-Constacyclic codes over $F_p + uF_p$ and their applications of constructing new non-binary quantum codes. *Quantum Inf. Process* **17**(4), (2018).

[4] KAI X., ZHU S., Quaternary construction of quantum codes from cyclic codes over $F_4 + uF_4$. *Int. J. Quantum Inform.* **9**, 689-700 (2011).

[5] QIAN J., Quantum codes from cyclic codes over $F_2 + vF_2$. *Journal of Inform.& computational Science* **16**(6), 1715-1722 (2013).

[1]Department of Mathematics
Ondokuz Mayıs University
Samsun, Turkey
abdullah.dertli@gmail.com

[2]Department of Mathematics
Trakya University
Edirne, Turkey
ycengellenmis@gmail.com

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Self-dual codes over chain rings

Simon Eisenbarth[1], **Gabriele Nebe**[1]

Let $\mathbb{F}$ be a finite field of characteristic p and $^- : \mathbb{F} \to \mathbb{F}$ be some automorphism of order one or two. A code C in $\mathbb{F}^n$ is called self-dual if it coincides with its dual code with respect to the standard Hermitian inner dot product

$$v \cdot w := \sum_{i=1}^{n} v_i \overline{w_i}.$$

In [4], upper bounds for the minimum distance of several families of self-dual codes were given. Self-dual codes which achieve those bounds are called extremal. In [1] and [2], a generel decomposition theory for self-dual codes over $\mathbb{F}$ admitting permutation automorphisms of order prime to p has been developed. This has been frequently used, for example to classify ternary extremal codes with an automorphism of prime order ≥ 5 (see [3], [5]). In a recent work (together with G. Nebe), we developed techniques to classify $\mathbb{F}$-linear, self-dual codes with an automorphism g of order $q = p^e$, where it can w.l.o.g. be assumed that $g \in S_n$.

The group ring $\mathbb{F}\langle g\rangle$ is an Artinian chain ring with ideals $\langle (1-g)^i\rangle,\ 0 \leq i \leq q$ and it carries a natural involution defined by

$$\overline{\sum_{i=0}^{q-1} \alpha_i g^i} := \sum_{i=0}^{q-1} \overline{\alpha_i} g^{-i}.$$

Our work focused on the case where g has no fix points on $\{1, \ldots, n = pt\}$ and C is a free $\mathbb{F}\langle g\rangle$-module. Then the map

$$\mathbb{F}^n \to \mathbb{F}\langle g\rangle^t, (c_1, \ldots, c_{pt}) \mapsto \left(\sum_{i=1}^{p} c_i g^{i-1}, \ldots, \sum_{i=1}^{p} c_{(t-1)p+i} g^{i-1} \right)$$

is a bijection between the self-dual codes in $\mathbb{F}^n$ and the self-dual codes in $\mathbb{F}\langle g\rangle^t$ with respect to an inner product defined in the next section. This motivated the analysis of the structure of self-dual codes over chain rings.

Let R be a commutative Artinian chain ring with 1 and let $^- : R \to R$ be an involution, i.e. a ring automorphism of order one or two. If $\mathfrak{m} \leq R$ denotes the maximal ideal of R, then $^-$ induces an involution of the residue field $\mathbb{F} = R/\mathfrak{m}$

which we again denote by $^-$. If this involution is the identity on the residue field, then there is $\epsilon \in \{1, -1\}$ such that $\overline{x} \equiv \epsilon x \pmod{Rx^2}$ for any generator x of $\mathfrak{m}$. If $^-$ has order 2 on $\mathbb{F}$ (which we refer to as the hermitian case) then by Hilbert 90 we may choose a generator x of $\mathfrak{m}$ such that $\overline{x} \equiv x \pmod{Rx^2}$. We fix such a generator x of the maximal ideal R such that

$$\overline{x} \equiv \epsilon x \pmod{Rx^2}$$

with $\epsilon = 1$ in the Hermitian case. Let $a \in \mathbb{N}_0$, such that

$$R \supset Rx \supset Rx^2 \supset \cdots \supset Rx^{a+1} = \{0\}$$

is the complete chain of ideals in R. Then all indecomposable R-modules are of the form

$$S_b := Rx^b \text{ for some } 0 \leq b \leq a$$

where $S_0 = R$ is the free module of rank 1 and S_a is the unique simple R-module. To consider codes let $t \in \mathbb{N}$ and

$$V := R^t = \{(v_1, \ldots, v_t) \mid v_i \in R\}$$

denote the free R-module of rank t. We define the $^-$-Hermitian standard inner product

$$\langle \cdot, \cdot \rangle : V \times V \to R, \langle v, w \rangle := \sum_{j=1}^{t} v_j \overline{w_j}.$$

on V. We call an R-submodule C of V a code of length t (over R). Then by the theorem of Krull, Remak, Schmidt, there are unique $t_0, t_1, \ldots, t_a \in \mathbb{Z}_{\geq 0}$ such that

$$C = S_0^{t_0} \oplus S_1^{t_1} \oplus \cdots \oplus S_a^{t_a}.$$

Now let $C = C^\perp$ be a self-dual code of even length t which is a free R-module, i.e. $t_0 = t/2$ and $t_1 = \cdots = t_a = 0$. Then the subcodes

$$C^{(i)} := Cx^i$$

form the following chain:

$$V = R^t \supset {C^{(a)}}^\perp \supset \cdots \supset {C^{(1)}}^\perp \supset C = C^\perp \supset C^{(1)} \supset \cdots \supset C^{(a)} \supset \{0\}.$$

We now want to iteratively construct the codes $C^{(a)}, C^{(a-1)}, \ldots, C$, starting with the socle $soc(C) = C^{(a)}$.

The multiplication by x^a defines an isomorphism between the residue field and the socle of R, and the map

$$\varphi : \mathbb{F} = R/Rx \xrightarrow{\sim} Rx^a = S_a, r + Rx \mapsto rx^a$$

can be naturally extended to the socle $soc(V) = Vx^a$ of V, i.e.

$$\pi : soc(V) \to \mathbb{F}^t, (v_1, \ldots, v_t) \mapsto (\varphi^{-1}(v_1), \ldots, \varphi^{-1}(v_t))$$

is an $\mathbb{F}$-linear isomorphism.
In our initial setting, this means that the fixcode of g is generated by some matrix

$$M \otimes \begin{pmatrix} 1 & \ldots & 1 \end{pmatrix},$$

where M generates a self-dual code in $\mathbb{F}^t$ with respect to the standard Hermitian inner product. Using the classification of self-dual codes of moderat lengths, one can therefore find all possibilities for $C^{(a)}$.

For the iteration process, let $0 \leq i < a$ and fix some $C^{(i+1)}$. We want to find all admissible $C^{(i)}$, i.e. all codes D which are self-orthogonal and $Dx = C^{(i+1)}$. We put

$$W_i := {C^{(i+1)}}^{\perp} x^i / C^{(i+1)} \cong \mathbb{F}^t$$

and define

$$(\cdot, \cdot)_i : W_i \times W_i \to \mathbb{F}, (Ax^i, Bx^i)_i := \varphi^{-1}(\langle A, B \rangle x^i).$$

Then $(\cdot, \cdot)_i$ is a well-defined, non-degenerate inner product which is Hermitian in the Hermitian case and $\epsilon^{(i+a)}$-symmetric bilinear otherwise.
With respect to this inner product, $X_i := (soc(V) + C^{(i+1)})/C^{(i+1)} \leq W_i$ is self-dual code $(W_i, (\cdot, \cdot)_i)$. Moreover, $C^{(i)}/C^{(i+1)}$ is a self-dual code as well that complements X_i, i.e.

$$W_i = C^{(i)}/C^{(i+1)} \oplus X_i.$$

By constructing all complements of X_i, we can find all lifts of $C^{(i+1)}$.

This theory has been used to show in an exhaustive search that every extremal ternary code of length 36 with an automorphism of order 3 is isomorphic to the Pless Code P_{36}, strengthening the result given in [3].

Keywords: Self-dual codes, automorphisms, chain ring

References

[1] W. C. HUFFMAN, On the [24,12,10] quaternary code and binary codes with an automorphism having two cycles. *IEEE Trans. Inform. Theory* **34**(3), 486–493 (1988).

[2] W. C. HUFFMAN, On extremal self-dual quaternary codes of lengths 18 to 28. I. *IEEE Trans. Inform. Theory* **36**(3), 651–660 (1990).

[3] W. C. HUFFMAN, On Extrema1 Self-Dual Ternary Codes of Lengths 28 to 40. *IEEE Transactions on Information Theory* **38**(4), 1395–1400 (1992).

[4] C. L. MALLOWS; N. J. A. SLOANE, An upper bound for self-dual codes. *Information and Control* **22**(2), 188–200 (1973).

[5] G. NEBE, On Extremal Self-Dual Ternary Codes of Length 48 *International Journal of Combinatorics* **2012**, (2012).

[1]Lehrstuhl D für Mathematik
RWTH Aachen University
52056 Aachen, Germany
simon.eisenbarth@rwth-aachen.de

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Constacyclic and Cyclic Codes over the Class of Finite Rings $\mathbb{F}_{2^k} + u\mathbb{F}_{2^k} + u^2\mathbb{F}_{2^k} + v\mathbb{F}_{2^k}$

G.Gozde GUZEL[1], **Abdullah DERTLI**[2], **Yasemin CENGELLENMIS**[3]

In this paper, a new class of finite rings includes the finite ring which is presented in [9] is given. It is shown that these rings are semilocal, principally ideal and Frobenious rings. It is studied the units and the ideals of the ring. It is introduced a Gray map on it. The Gray images of both cyclic and $(1 + u)$-constacyclic codes over the finite ring are obtained.

Keywords: Gray map, Cyclic codes, Quasicyclic codes

References

[1] M.C.V. AMARRA, AND F.R. NEMENZO, On $(1 - u)-$ cyclic codes over $F_{p^k} + uF_{p^k}$,*Appl. Math. Lett.*, **21**, 1129–1133, (2008).

[2] N. AYDIN, Y.CENGELLENMIS, A. DERTLI, On some constacyclic codes over $Z_4[u]/(u^2 - 1)$, their Z_4 images, and new codes, *Des. Codes Cryptogr.*, DOI 10.1007/s10623-017-0392-y, (2017).

[3] I.F.BLAKE, Codes over certain rings, *Inform. Control*, **20**, 396–404, (1972).

[4] I.F.BLAKE, Codes over integer residue rings, *Inform. Control*, **29**, 295–300,(1975).

[5] Y. CENGELLENMIS, On $(1 - u^m)-$cyclic codes over $F_2 + uF_2 + u^2F_2 + ... + u^mF_2$, *International Journal of Contemporary Math. Sci.*, **4** 987–992, (2009).

[6] A. DERTLI, Y. CENGELLENMIS, On $(1+u)-$cyclic and cyclic codes over $F_2 + uF_2 + vF_2$, *European J. of Pure and Applied Math.*, **9**, 305–313, (2016).

[7] S.T. DOUGHERTY, E.SALTURK, Constacyclic codes over local rings of order 16, to be submitted.

[8] J. GAO, Linear codes and $(1 + uv)-$constacyclic codes over $R[v]/(v^2 + v)$, *IEICE Transactions on Fundamentals* , **E98-A**, 1044–1048,(2015).

[9] GUZEL G.G., DERTLI A., CENGELLENMIS Y., The $(1 + u^2)-$ constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + v\mathbb{F}_2$, to be submitted.

[10] A.R. HAMMONS JR., P.V.KUMAR, A.R.CALDERBANK, N.J.A. SLOANE, P. SOLÉ, *The Z_4- linearity of Kerdock, Preparata, Goethal, and related codes*, IEEE Trans. Inform. Theory, **40**, 301–319, (1994).

[11] X.KAI, S.ZHU, L. WANG, A family of constacyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$, J Sysst Sci Complex,**25**, 1032–1040,(2012).

[12] S. KARADENIZ, B. YILDIZ, $(1 + v)-$constacyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$, Journal of Franklin Ins., **348**, 2625–2632, (2011).

[13] D. LIAO, Y. TANG, A class of constacyclic codes over $R+vR$ and its Gray image, Int. J. Communications, Network and System Sciences, **5**, 222–227,(2012).

[14] J.F. QIAN, L.N.ZANG, S.X. ZHU, $(1+u)-$constacyclic and cyclic codes over $F_2 + uF_2$, Appl. Math. Lett., **19**, 820–823, (2006).

[15] J.F. QIAN, L.N.ZANG, S.X. ZHU, Constacyclic and cyclic codes over $F_2 + uF_2 + u^2F_2$, IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, **E89-A(6)**, 1863–1865, (2006).

[16] S. ZHU, L. WANG, A class of constacyclic codes over $F_p + vF_p$ and its Gray image , Discrete Mathematics, **311**, 2677–2682,(2011).

[1]Ipsala Vocational College
Trakya University
Edirne, Turkey
ggozdeguzel@gmail.com

[2]Department of Mathematics, Faculty of Arts and Sciences
Ondokuz Mayis University
Samsun,Turkey
abdullah.dertli@gmail.com

[3]Department of Mathematics, Faculty of Science
Trakya University
Edirne, Turkey
ycengellenmis@gmail.com

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Cyclic structures in convolutional codes and free distance*

José Gómez-Torrecillas[1], **F. J. Lobillo**[1], **Gabriel Navarro**[2]

The results of this talk are included in [6].

A rate k/n convolutional code $\mathcal{C}$ over a finite field $\mathbb{F}$ can be modeled as a rank k direct summand of $\mathbb{F}[z]^n$, i.e. $\mathcal{C} = \mathrm{im}(\cdot G)$ where $G = \sum_{i=0}^{m} z^i G_i \in \mathcal{M}_{k\times n}(\mathbb{F}[z])$ is basic. One of the main parameters of convolutional codes is the free distance, which is directly related with the correction capability of a convolutional code. The free distance is defined as

$$\mathrm{d}_{\mathsf{free}}(\mathcal{C}) = \min\left\{\mathrm{w}_{\mathsf{H}}(f) : f \in \mathcal{C}, f \neq 0\right\},$$

see [7, Ch. 3], where the Hamming weight of a polynomial over $\mathbb{F}^n$ is the coefficient-wise extension of the Hamming weight in $\mathbb{F}^n$. The free distance of a convolutional code can be calculated computing the classic associated column and row distances until they coincide. Both sequences must be computed since there is not regularity in their respectively increase and decrease.

Cyclic structures on convolutional codes can be provided enriching the algebraic structure of $\mathbb{F}^n$. Concretely, let A be an n-dimensional $\mathbb{F}$-algebra, $\sigma : A \to A$ an $\mathbb{F}$-automorphism and $\mathfrak{v} : A[z;\sigma] \to \mathbb{F}^n[z]$ the canonical isomorphism associated to a fixed basis of A. A convolutional code $\mathcal{C}$ is said to be skew cyclic, see [2], if $\mathcal{C} = \mathfrak{v}(I)$ for some left ideal $I \leq A[z;\sigma] = R$. If, in addition, I is a direct summand as left ideal, i.e. $I = R(1-e) = \mathrm{Ann}_R^{\ell}(e)$ for some idempotent $e = \sum_{i=0}^{m} z^i e_i \in R$, then $\mathcal{C}$ is called an idempotent convolutional code, see [4, 5].

Let

$$E_k^c = \left[\sigma^{-j}(e_{j-i})\right]_{0\leq i,j\leq k} \in \mathcal{M}_{k+1}(A).$$

We introduce the kth cyclic column distance of $\mathcal{C}$ as

$$\delta_k^c = \min\left\{\mathrm{w}(a_0,\ldots,a_k) \mid (a_0,\ldots,a_k) \in \ker(\cdot E_l^c), a_0 \neq 0\right\}.$$

The main result of this talk is

Theorem. *Let A be an n-dimensional $\mathbb{F}$-algebra and let σ be an isometry on A with respect to a fixed basis. Let $R = A[z;\sigma]$ and $\mathfrak{v} : R \to \mathbb{F}^n[z]$. Let $\mathcal{C} = \mathfrak{v}(\mathrm{Ann}_R^{\ell}(e))$ for some idempotent $e = \sum_{i=0}^{m} z^i e_i \in R$. Let E_k^c and δ_k^c be as before. Then $\delta_k^c \leq \delta_{k+1}^c \leq \mathrm{d}_{\mathsf{free}}\mathcal{C}$. If $\delta_k^c = \delta_{k+m}^c$, then $\mathrm{d}_{\mathsf{free}}(\mathcal{C}) = \delta_k^c$.*

The theorem allows to compute the free distance by using the cyclic column distance sequence. No row distance is needed.

*Research partially supported by grant MTM2016-78364-P from Agencia Estatal de Investigación and from FEDER.

Keywords: Cyclic convolutional code, Free distance

References

[1] S. Estrada, J. R. García-Rozas, J. Peralta, and E. Sánchez-García. 2008. Group convolutional codes. *Advances in Mathematics of Communications* 2, 1 (2008), 83–94. https://doi.org/10.3934/amc.2008.2.83

[2] H. Gluesing-Luerssen and W. Schmale. 2004. On Cyclic Convolutional Codes. *Acta Applicandae Mathematicae* 82, 2 (2004), 183–237. https://doi.org/10.1023/B:ACAP.0000027534.61242.09

[3] J. Gómez-Torrecillas, F. J. Lobillo, and G. Navarro. 2016a. Convolutional codes with a matrix-algebra word ambient. *Advances in Mathematics of Communications* 10, 1 (2016), 29–43.

[4] J. Gómez-Torrecillas, F. J. Lobillo, and G. Navarro. 2017b. Ideal codes over separable ring extensions. *IEEE Transactions on Information Theory* 63, 5 (May 2017), 2796 – 2813. https://doi.org/10.1109/TIT.2017.2682856

[5] J. Gómez-Torrecillas, F. J. Lobillo, and G. Navarro. 2017a. Computing separability elements for the sentence-ambient algebra of split ideal codes. *Journal of Symbolic Computation* 83 (2017), 211–227.

[6] J. Gómez-Torrecillas, F. J. Lobillo, and G. Navarro. 2018. Computing free distances of idempotent convolutional codes. In *Proceedings of the 2018 ACM on International Symposium on Symbolic and Algebraic Computation (ISSAC '18)*. ACM, New York, NY, USA.

[7] R. Johannesson and K. Sh. Zigangirov. 1999. *Fundamentals of Convolutional Coding*. Wiley-IEEE Press. http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0780334833,miniSiteCd-IEEE2.html

[8] S. R. López-Permouth and S. Szabo. 2013. Convolutional codes with additional algebraic structure. *Journal of Pure and Applied Algebra* 217, 5 (2013), 958 – 972. https://doi.org/10.1016/j.jpaa.2012.09.017

[9] P. Piret. 1976. Structure and constructions of cyclic convolutional codes. *IEEE Transactions on Information Theory* 22, 2 (1976), 147–155. https://doi.org/10.1109/TIT.1976.1055531

[1]CITIC and Department of Algebra
University of Granada
E18071 Granada
Spain
gomezj@ugr.es
jlobillo@ugr.es

[2]CITIC and Department of Computer Science and Artificial Intelligence
University of Granada
E18071 Granada
Spain
gnavarro@ugr.es

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Generalized Hamming Weights of Binary Linear Codes

I. Márquez-Corbella[1], **E. Martínez-Moro**[2]

We can associate to each linear code $\mathcal{C}$ defined over a finite field the matroid $M[H]$ of its parity check matrix H. For any matroid M one can define its generalized Hamming weights which are the same as those of the code $\mathcal{C}$. In [1] the authors show that the generalized Hamming weights of a matroid are determined by the $\mathbb{N}$-graded Betti numbers of the Stanley-Reisner ring of the simplicial complex whose faces are the independent set of M. In this talk we go a step further. Our practical results indicate that the generalized Hamming weights of a linear code $\mathcal{C}$ can be obtained from the monomial ideal associated with a test-set for $\mathcal{C}$. Moreover, recall that in [2] we use the Gröbner representation of a linear code $\mathcal{C}$ to provide a test-set for $\mathcal{C}$.

Our results are still a work in progress, but its applications to Coding Theory and Cryptography are of great value.

Keywords: Generalized Hamming Weights, Test Set

References

[1] J. T. Johnsen and H. Verdure. *Hamming weights and Betti numbers of Stanley–Reisner rings associated to matroids*. Applicable Algebra in Engineering, Communication and Computing. 24(1): 73-93, 2013.

[2] I. Márquez-Corbella, E. Martínez-Moro and E. Suárez-Canedo. *On the ideal associated to a linear code*. Advances in Mathematics of Communications (AMC). 10(2): 229-254, 2016.

[1]Department of Mathematics, Statistic and O. Research
University of La Laguna, Spain
imarquec@ull.edu.es

[2]Mathematics Research Institute
University of Valladolid, Castilla, Spain
edgar.martinez@uva.es

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

On additive cyclic codes over chain rings

E. Martínez-Moro[1], **K. Otal**[2] and **F. Özbudak**[2]

Additive codes are a direct and useful generalization of linear codes, and they have applications in quantum error correcting codes. There are several studies using different approaches on them and their applications. On the other hand cyclic codes are one of the most attractive code families thanks to their rich algebraic structure and easy implementation properties. In this talk we will investigate the structure of Additive cyclic codes over finite (commutative) chain rings. When we focus on non-Galois finite commutative chain rings, we observe two different kinds of additivity. One of them is a natural generalization of precedding studies whereas the other one has some unusual properties especially while constructing dual codes. We interpret the reasons of such properties and illustrate our results giving concrete examples.

Keywords: Cyclic codes, Additive codes, Codes over rings

References

[1] EDGAR MARTÍNEZ-MORO,KAMIL OTAL,FERRUH ÖZBUDAK, Additive cyclic codes over finite commutative chain rings. *Discrete Mathematics* **(341-7)**, 1873–1884 (2018).

[1]Mathematics Research Institute
University of Valladolid, Castilla, Spain
edgar.martinez@uva.es

[2]Department of Mathematics and Institute of Applied Mathematics
Middle East Technical University, Ankara, Turkey
kamil.otal@gmail.com
ozbudak@metu.edu.tr

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

On varieties and codes defined by quadratic equations

Ruud Pellikaan[1]

We will review the work on algebraic geometry codes $\mathcal{C} = \mathcal{C}_L(\mathcal{X}, P, E)$ that have a unique representation $(\mathcal{X}, P, E)$, where $\mathcal{X}$ is an algebraic curve, P is an n-tuple of mutually distinct points and E is a divisor. See [1, 2, 4, 5]. As a consequence algebraic geometry codes with certain parameters are not secure for the code based McEliece public crypto system.

One of the key ingredients of these results is the classical fact that certain curves embedded in projective space are defined by quadratic equations. We consider generalizations to higher dimensional varieties [6] and order domains [3] and their corresponding codes.

Keywords: McEliece public crypto system, algebraic geometry codes

References

[1] A. Couvreur, I. Márquez-Corbella and R. Pellikaan, "Cryptanalysis of public-key cryptosystems that use subcodes of algebraic geometry codes". In *Coding theory and applications*, pp. 133—140, CIM Ser. Math. Sci., 3, Springer, Cham, 2015.

[2] A. Couvreur, I. Márquez-Corbella and R. Pellikaan, "Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes". IEEE Trans. Inform. Theory vol. 63, pp. 5404—5418, 2017.

[3] O. Geil and R. Pellikaan, "On the structure of order domains". Finite Fields Appl. vol. 8, pp. 369-–396, 2002.

[4] I. Márquez-Corbella, E. Martínez-Moro and R. Pellikaan, "On the unique representation of very strong algebraic geometry codes". Designs, Codes and Cryptography, vol.70, pp. 215—-230, 2014.

[5] I. Márquez-Corbella, E. Martínez-Moro, D. Ruano and R. Pellikaan, "Computational aspects of retrieving a representation of an algebraic geometry code", J. Symbolic Comput. vol. 64, pp. 67—87, 2014.

[6] D. Mumford, "Varieties defined by quadratic equations". In: *Questions on Algebraic Varieties*, C.I.M.E., III Ciclo, Varenna, 1969, pp. 29—100. Edizioni Cremonese, Rome 1970.

[1]Department of Mathematics and Computing Science
Technical University of Eindhoven
g.r.pellikaan@tue.nl

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Computer algebra tales on Goppa codes and McEliece cryptography

Narcís Sayols[1], **Sebastià Xambó-Descamps**[2]

Abstract

The fourty-year old McEliece public-key crypto-system is revisted with the help of recently developed resources: an improved Peterson-Gorenstein-Zierler decoder for alternant error-correcting codes; PyECC, a purely Python CAS; a package of PyECC functional utilities for the computations involved in defining, coding and decoding error-correcting codes; a web page with free-access to the materials generated by the project.

Keywords: Error-correcting codes, Classical Goppa codes, Post-quantum cryptography

One of the motivations for this work was the development of a purely Python CAS environment to cover the computational needs of a book such as [11] and the confidence gained in implementing decoders like the old Peterson-Gorenstein-Zierler [7, 3, 8], including the improvements presented in [2], and the computations for [5]. Further developments led to the CAS system that is now available at https://mat-web.upc.edu/people/sebastia.xambo/PyECC.htmlPyECC. The revisiting of the McEliece public-key crypto-system [4], which is based in a class of binary classical Goppa codes, was a further test of these tools. One friendly feature of the environment is the availability of the source code through Jupyter notebooks.*

The main purpose of our talk is to present an overview of those developments and will be structured as follows: A brief introduction to Goppa codes, particularly to their decoding (see [11, 2]); a detailed description of the McEliece system [4] and analysis of its security levels (see [1, 6]); a report on the structure and functionality of PyECC, with emphasis on the utilities needed for the implementation of that system.

References

[1] D. J. Bernstein, T. Lange, and C. Peters. Attacking and defending the McEliece cryptosystem. In PQCrypto '08: Proceedings of the 2nd International Workshop on Post-Quantum Cryptography, Lecture Notes in Computer Science, pages 31-46. Springer, 2008.

*http://jupyter.org/

[2] R. Farré, N. Sayols, and S. Xambó-Descamps. On the PGZ decoding algorithm for alternant codes. arXiv:1704.05259, 2017.

[3] D. Gorenstein and N. Zierler. A class of error-correcting codes in p^m symbols. *J. Soc. Ind. Appl. Math.* 9(2):207–214, 1961.

[4] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory, 1978. Jet Propulsion Laboratory DSN Progress Report 42-44. URL: `http://ipnpr.jpl.nasa.gov/progressreport2/42-44/44N.PDF`.

[5] S. Molina, N. Sayols, S. Xambó-Descamps. A bootstrap for the number of $\mathbb{F}_{q^m}$-rational points on a curve over $\mathbb{F}_q$. https://arxiv.org/pdf/1704.04661.pdfarXiv

[6] R. Niebuhr. *Attacking and Defending Code-based Cryptosystems*. https://d-nb.info/1106116461/34PhD thesis, 2012.

[7] W. W. Peterson. Encoding and error-correction procedures for the Bose-Chaudhuri codes. *IRE Transactions on Information Theory*, IT-6:459-470, 1960.

[8] W. W. Peterson and E. J. Weldon. *Error-Correcting codes*. MIT Press (2nd edition), 1972.

[9] J. Rué, S. Xambó-Descamps. Introducció matemàtica a la computació quàntica, *Butlletí de la Societat Catalana de Matemàtiques*, 28/2 (2013), 183-231.

[10] N. Sayols and S. Xambó-Descamp. A Python package for the construction, coding and decoding of error-correcting codes. https://mat-web.upc.edu/people/sebastia.xambo/PyECC.htmlPyECC, 2017.

[11] S. Xambó-Descamps. *Block error-correcting codes: a computational primer*. Univesitext. Springer, 2003.

[12] S. Xambó-Descamps, N. Sayols. Alternant codes and the McEliece cryptosystem. https://mat-web.upc.edu/people/sebastia.xambo/PyECC/s-CryptoLleida-7-10-2017.pdfpdf

[1]Departament d'Enginyeria de Sistemes, Automàtica i Informàtica Industrial
Universitat Politècnica de Catalunya
Jordi Girona, 1-3. K2M
narcissb@gmail.com

[2]Department de Matemàtiques
Universitat Politècnica de Catalunya
Jordi Girona, 1-3. Omega
sebastia.xambo@upc.edu

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

On the rank and kernel of new HFP-codes

E. Suárez-Canedo[1]

Hadamard codes with a subjacent group structure were principally studied from the point of view of cocyclic Hadamard matrices, Hadamard groups, and relative difference sets [1, 2, 3]. Propelinear codes, introduced in 1989 [4], also played an important role on the computation of Hadamard codes; indeed, they allow to classify Hadamard codes with a subjacent $\mathbb{Z}_2\mathbb{Z}_4$ and $\mathbb{Z}_2\mathbb{Z}_4Q_8$ group structure attending to the values of the rank and dimension of the kernel [5]. In [6] we define the family of HFP-codes and we prove the equivalences between them and Hadamard groups. Furthermore, constructions on HFP-codes with a subjacent $C_n \times Q_8$ and the dicyclic Q_{8n} group structure appear in [7, 8]. Now we classify new families of HFP-codes attending to the values of the rank and dimension of the kernel.

Keywords: Rank, kernel, HFP-codes.

References

[1] A. T. BUTSON, *Generalized Hadamard matrices,* Proc. Amer. Math. Soc., vol. 13, pp. 894-898, 1962.

[2] K. J. HORADAM, W. DE LAUNEY, *Generation of cocyclic Hadamard matrices,* Research Report No. 2, Mathematics Department, RMIT, March 1993.

[3] N. ITO, *On Hadamard groups,* J. Algebra 168, pp. 981-987, 1994.

[4] J. RIFÀ, J. M. BASART, L. HUGUET, *On Completely regular propelinear codes,* AAECC-6 Proc. of the 6th International Conference, on Appl. Algebra, Alg. Algorithms and Error-Correcting Codes, pp. 341-355, 1989.

[5] A. DEL RIO, J. RIFÀ, *Families of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-codes,* IEEE Trans. Inf. Theory, vol. 59, no. 8, pp. 5140–5151, 2013.

[6] J. RIFÀ, E. SUÁREZ-CANEDO, *About a class of Hadamard propelinear codes,* Electron. Note Discr. Math., vol. 46, pp. 289-296, 2014.

[7] J. RIFÀ, E. SUÁREZ-CANEDO, *Kronecker sums to construct Hadamard full propelinear codes,* Proc. of the 21-st Conference on applications of Computer Algebra (ACA15), Kalamata, Greece, pp. 135-139, 20-23 July 2015.

[8] J. RIFÀ, E. SUÁREZ-CANEDO, *Hadamard full propelinear codes of type Q; rank and kernel,* E. Des. Codes Cryptogr. (2017). https://doi.org/10.1007/s10623-017-0429-2

[1]Departament d'Enginyeria de la Informació i les Comunicacions
Universidad Autónoma de Barcelona, Spain
emiliosuarezcanedo@gmail.com

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Satisfiability modulo theory in finding the distance distribution of binary constrained arrays

Putranto Utomo[1]

Despite of the hardness of finding the distance distribution of a code, it is one of the important topics in coding theory. By knowing the distance distribution of a code, we can measure the performance of the code.

The development in satisfiability (SAT) theory has been improved recently. The modern SAT solver is performing much better in terms of computational efficiency. Unfortunately not all problems could easily be expressed as a propositional satisfiability problem, and some could lead to a very complex representation. This problem gives rise to a new topic called satisfiability modulo theory (SMT). The idea is to restrict the fragment of first order logic to some logical background theory. By doing this, it can solve more varied problems efficiently using the SAT solver engine.

The constrained system, especially the 1-D constraint, has proved to be beneficial for the magnetic tape recording. Recent developments in data recording technology allows us to store data in 2-D format, such as the holographic recording technology. However, in contrast with the constrained sequence, the theory is not yet well developed.

In this paper, we utilize the power of the SMT solver to find the distance distribution of 2-D binary constrained systems.

Keywords: Constrained arrays, Distance distribution

[1]Department of Mathematics and Computer Science
Eindhoven University of Technology
Posbus 513. 5600MB Eindhoven
p.h.utomo@tue.nl

S10
Parametric Polynomial Systems

Parametric polynomial system solving is a challenge coming from many applications, such as biology, control theory, robotics, deformation of hypersurface singularities, etc. When a problem can be modelled by a parametric system, the main issue is not only to return its solutions, but also to describe them. The design of algorithms to solve parametric systems has recently become an active and expanding research field. Manipulating parametric systems is at the heart of computer algebra. It calls upon a wide range of methods, such as comprehensive Gröbner bases, Cylindrical Algebraic Decomposition, Quantifier Elimination, Comprehensive Triangular Sets, Comprehensive Involutive Systems, Parametric Local Cohomology System, etc.

This session is focused on the art of parametric system solving, for general class of systems or dedicated to specific application problems, including the following topics:

- Comprehensive Gröbner bases (systems)
- Quantifier elimination
- Comprehensive triangular sets
- Deformation of hypersurface singularities
- Modelisation of parametric problems
- Optimization of parametric systems
- Resolution of sparse parametric systems
- Low-level computation with multivariate polynomial coefficients
- Resolution of polynomial systems with boolean parameters
- Description of the real solutions of a parametric system
- Description of the parameter space of a polynomial system
- Extension of algorithms from non parametric to parametric systems

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

An overview on marked bases and applications

Cristina Bertone[1]

The Hilbert scheme was introduced by Grothendieck in the 60s. One can simply think of the Hilbert scheme $\mathrm{Hilb}^{\mathrm{n}}_{\mathrm{p(t)}}$ as a set containing all the saturated homogeneous ideals I in a certain polynomial ring $\Bbbk[x_0,\ldots,x_n] = \Bbbk[\mathbf{x}]$, with $\Bbbk$ a field, such that $\Bbbk[\mathbf{x}]/I$ has a given Hilbert polynomial $p(t)$. Grothendieck proved that $\mathrm{Hilb}^{\mathrm{n}}_{\mathrm{p(t)}}$ is not just a set, but it has a projective scheme structure. Although expert researchers investigated it, the Hilbert scheme is a mysterious object. Few properties are known, for instance Hartshorne proved connectedness in his Ph.D. Thesis.

A natural appealing application of Gröbner bases in Algebraic Geometry is the possibility to investigate families of ideals, and understand whether there is a scheme parameterizing them. In this framework, several authors tried to investigate the Hilbert Scheme by Gröbner techniques, see for instance [8]. The family of ideals having a certain initial ideal J for a given term order $\prec$ is called *Gröbner Stratum*. Imposing conditions for a suitable monic set of parametric polynomials to be a Gröbner basis gives the structure of closed scheme to the Gröbner Stratum of J in an affine space. Applying this construction to $J_{\geq r}$, where J is a monomial ideal such that $\Bbbk[\mathbf{x}]/J$ has Hilbert polynomial $p(t)$ and r is the Gotzmann number of $p(t)$, one can obtain a stratification of the Hilbert scheme by means of Gröbner Strata. Each of these Gröbner Strata is isomorphic to a locally closed subset (in general not an open subset) of $\mathrm{Hilb}^{\mathrm{n}}_{\mathrm{p(t)}}$ [8, Theorem 6.3 (i)].

From the point of view of Algebraic Geometry, the fact that a Gröbner Stratum is not in general an open subset of $\mathrm{Hilb}^{\mathrm{n}}_{\mathrm{p(t)}}$ is a big issue. This means that Gröbner Strata are not suitable to locally study $\mathrm{Hilb}^{\mathrm{n}}_{\mathrm{p(t)}}$. Furthermore, it is not possible to obtain the ring of coordinates of $\mathrm{Hilb}^{\mathrm{n}}_{\mathrm{p(t)}}$, as a subscheme of a suitable projective space, by "glueing" the affine schemes of the Gröbner Strata that cover $\mathrm{Hilb}^{\mathrm{n}}_{\mathrm{p(t)}}$.

In order to overcome the flaws of Gröbner strata with respect to the investigation of Hilbert schemes, a successful idea is to replace the use of a term order by considering special monomial ideals with strong combinatorial structure. Geometrically, it is totally reasonable to focus on this sort of monomial ideals: for instance Hartshorne proved the connectedness of the Hilbert scheme using *strongly stable* monomial ideals.

We construct families of ideals by suitable parametric polynomial generators which are monic in the terms generating a *quasi-stable ideal*. By imposing condition on these generators in order to have a *marked basis*, we describe an open subset of $\mathrm{Hilb}^{\mathrm{n}}_{\mathrm{p(t)}}$ around the quasi-stable ideal.

1 Marked bases over a quasi-stable ideal

Here is a summary of the construction of marked bases over a quasi-stable ideal. The main references are [4, 7, 1].

Assume that $x_0 > \cdots > x_n$. If σ is a term, we denote by $\min(\sigma)$ (resp. $\max(\sigma)$) the index of the smallest (resp. biggest) variable dividing σ. We choose a *quasi-stable* monomial ideal $J \subset \Bbbk[\mathbf{x}]$. This monomial ideal has a special set of monomial generators, a *Pommaret basis* $\mathcal{P}(J)$, such that: for every $\sigma \in J$, there is a unique $\eta \in \mathcal{P}(J)$ such that $\sigma = \eta \cdot \delta$ where δ is a term and $\min(\eta) \geq \max(\delta)$.

Let A be a Noetherian $\Bbbk$-algebra. We construct a *set of (monic) marked polynomials over* J, $G_{\mathcal{P}(J)}$, in the following way: for every $\eta \in \mathcal{P}(J)$, we define $f_\eta := \eta - \sum_{\tau \notin J} c_{\eta\tau}\tau$, where $c_{\eta\tau} \in A$. The term η is the *head term* of f_η. The set $G_{\mathcal{P}(J)}$ is a *marked basis* if the terms of degree s outside J are a basis of the module $A[\mathbf{x}]_s/(G_{\mathcal{P}(J)})_s$, for every s. Thanks to the quasi-stability of J, it is possible to define a polynomial reduction process.

Definition 8. *We denote by* $\xrightarrow{G_{\mathcal{P}(J)}}$ *the transitive closure of the following reduction relation in* $A[\mathbf{x}]$*: g and g' are in relation if $g' = g - c\delta f_\eta$, with $\delta\eta \in J$ is a term appearing in g with coefficient $c \neq 0_A$, f_η belongs to $G_{\mathcal{P}(J)}$, δ is a term and* $\min(\eta) \geq \max(\delta)$.

The reduction $\xrightarrow{G_{\mathcal{P}(J)}}$ is Noetherian and confluent: for every $g \in A[\mathbf{x}]$, there is a unique h such that $g \xrightarrow{G_{\mathcal{P}(J)}} h$ and every term appearing with non-zero coefficient in h does not belong to J (the support of h is outside J).

Theorem 9. *[Buchberger-like criterion] For every $\eta \in \mathcal{P}(J)$, for every $i > \max(\eta)$, we compute $h_{\eta,i}$ such that $x_i f_\eta \xrightarrow{G_{\mathcal{P}(J)}} h_{\eta,i}$ and the support of $h_{\eta,i}$ is outside J. $G_{\mathcal{P}(J)}$ is a marked basis over J if and only if $h_{\eta,i} = 0$ for every $\eta \in \mathcal{P}(J)$, for every $i > \min(\eta)$.*

We can construct a marked set $\mathcal{G}_{\mathcal{P}(J)}$, replacing $c_{\eta\tau} \in A$ by a parameter $C_{\eta\tau}$. Let C be the set of paramters $C_{\eta\tau}$. By Theorem 9, we impose conditions in $\Bbbk[C]$ for $\mathcal{G}_{\mathcal{P}(J)}$ to be a marked basis: in this way we obtain a *marked scheme*. More precisely:

Theorem 10. *For every $\eta \in \mathcal{P}(J)$, for every $i > \min(\eta)$, compute $h_{\eta,i}$ as in Theorem 9. Let $\mathcal{R} \subset \Bbbk[C]$ be the ideal generated by the $\mathbf{x}$-coefficients of the polynomials $h_{\eta,i}$. The affine scheme $\mathrm{M}_{\mathcal{P}(J)} := \mathrm{Spec}(\Bbbk[C]/\mathcal{R})$ paramaterizes the ideals in $A[\mathbf{x}]$ generated by a marked basis over J, for every Noetherian $\Bbbk$-algebra A. We call* $\mathrm{M}_{\mathcal{P}(J)}$ marked scheme over J.

Marked schemes give an *open cover* of $\mathrm{Hilb}^{\mathrm{n}}_{\mathrm{p(t)}}$ as follows. We compute the complete list L of saturated quasi-stable ideals J having Hilbert polynomial $p(t)$, and for each of them we compute the marked scheme over $J_{\geq r}$, where r is the *Gotzmann number* of $p(t)$. Each of these marked schemes is an open subset of $\mathrm{Hilb}^{\mathrm{n}}_{\mathrm{p(t)}}$ [7,

Theorem 1.13].
Furthermore, we consider the usual action of $\mathrm{PGL} = \mathrm{PGL}_{\Bbbk}(\mathrm{n}+1)$ on $A[\mathbf{x}]$, and extend it to the points of $\mathrm{Hilb}^{\mathrm{n}}_{\mathrm{p(t)}}$. Up to this action of PGL, we get an open cover of $\mathrm{Hilb}^{\mathrm{n}}_{\mathrm{p(t)}}$ by means of the computed marked schemes [7, Theorem 2.5]:

$$\mathrm{Hilb}^{\mathrm{n}}_{\mathrm{p(t)}} = \bigcup_{g\in\mathrm{PGL}, J\in L} g\cdot \mathrm{M}(J_{\geq r}). \tag{1}$$

This open cover is actually *functorial*: the marked schemes glue together, and it is possible to explicitely compute equations that define the projective scheme $\mathrm{Hilb}^{\mathrm{n}}_{\mathrm{p(t)}}$ in a suitable projective space. This gives a new proof of the existence of the Hilbert scheme. The complete proof is in [6] for the Hilbert scheme, in [2] for the locus with bounded regularity, and in [1] this is generalized to Quot Schemes.

2 Some Applications

(1) The parametric system of equations we use to compute the conditions in $\Bbbk[C]$ for a marked basis is also used in order to study the liftings of a projective scheme. In [3], we prove that the liftings of a projective scheme with a given Hilbert polynomial are parameterized by a closed subscheme of a union of some marked schemes. Although Gröbner strata are sufficient to complete a first part of the investigation (x_n-liftings), marked schemes turn out to be the suitable approach to geometric liftings, due to the reasonable geometric assumption that the scheme to lift is in general position and to the openness of marked schemes in $\mathrm{Hilb}^{\mathrm{n}}_{\mathrm{p(t)}}$.
(2) We can use marked schemes as open neighbourhoods of interesting points of $\mathrm{Hilb}^{\mathrm{n}}_{\mathrm{p(t)}}$, not only those defined by monomial ideals: for instance, we use them in [5] in order to prove the smoothability of the Gorenstein graded $\Bbbk$-algebras with Hilbert function $(1,7,7,1)$ (and as a byproduct of the computations we obtain that Hilb^{7}_{16} has at least 3 irreducible components).
(3) As already mentioned, from the open cover (1), it is possible to compute the equations defining the Hilbert scheme as a subscheme of a suitable projective space [6]. This construction is generalized in [2] for the locus with bounded regularity, and in [1] to the case of Quot Schemes. These equations allow the direct study of Hilbert and Quot schemes. For instance, a paper on the Quot scheme of modules in $\Bbbk[x,y]^2$ with Hilbert polynomial $p(z)=2$ is in progress.

Keywords: quasi-stable ideal, polynomial reduction process, Hilbert scheme

References

[1] M. ALBERT; C. BERTONE; M. ROGGERO; W.M. SEILER, Marked bases over quasi-stable modules and quot schemes, *in progress, preliminar version at arXiv:1511.03547*.

[2] E. BALLICO; C. BERTONE; M. ROGGERO, The locus of points of the Hilbert scheme with bounded regularity, *Comm. Algebra* **43**, no. 7, 2912–2931 (2015).

[3] C. BERTONE; F. CIOFFI; D. FRANCO, Functors of liftings of projective schemes, *preprint available at arXiv:1706.02618*.

[4] C. BERTONE; F. CIOFFI; P. LELLA; M. ROGGERO, Upgraded methods for the effective computation of marked schemes on a strongly stable ideal, *J. Symbolic Comput.* **50**, 263–290 (2013).

[5] C. BERTONE; F. CIOFFI; M. ROGGERO, Smoothable gorenstein points via marked schemes and double-generic initial ideals, *preprint available at arXiv:1712.06392*.

[6] J. BRACHAT; P. LELLA; B. MOURRAIN; M. ROGGERO, Extensors and the Hilbert scheme, *Ann. Sc. Norm. Super. Pisa Cl. Sci.* (5) **16**, no. 1, 65–96 (2016).

[7] C. BERTONE; P. LELLA; M. ROGGERO, A Borel open cover of the Hilbert scheme, *J. Symbolic Comput.* **53**, 119–135 (2013).

[8] P. LELLA; M. ROGGERO, Rational components of Hilbert schemes. *Rend. Semin. Mat. Univ. Padova* **126**, 11–45 (2011).

[1]Dipartimento di Matematica “G. Peano”,
Università di Torino
via Carlo Alberto 10, 10123 Torino, Italy
cristina.bertone@unito.it

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Fitting a Sphere to Point Cloud Data via Computer Algebra

Robert H. Lewis[1], **B. Paláncz**[2] **J. Awange**[3]

To determine orientation using different kinds of sensors requires reference objects. One of the most frequently employed reference object is a sphere with known radius R and center coordinates (x, y, z).

In this paper we investigate the identification of these parameters from point cloud data contaminated by outliers and corrupted by low sensor resolution. Our main tools are Gröbner basis and the Dixon resultant. First the deterministic subsystems of the overdetermined system are solved. Algebraic computations show that when R is known, but the center coordinates are unknown, the algebraic and geometric fittings provide two solutions, while in the case of unknown R, the geometric fitting gives a unique solution.

The raw data of the point cloud were filtered using a Self Organized Map neural network. The overdetermined system was solved via a simplified Gauss-Jacobi technique using the results of the algebraic computations. This involves a polynomial system with 20 parameters. Our method is illustrated by a symbolic-numeric example based on real field measurement data using *Mathematica* and *Fermat* computer algebra systems.

Keywords: point cloud, polynomial system, resultant, symbolic-numeric, Gröbner basis

References

[1] J. AWANGE, B. PALÁNCZ, R. LEWIS, Groebner Basis in Geodesy and Geoinformatics. in *Mathematical Software ICMS 2014, LNCS 8592*, pp 359 - 366. Springer Verlag, New York. 2014.

[2] J. AWANGE, B. PALÁNCZ, R. LEWIS, Y. FUKUDA, T. LOVAS, An Algebraic solution of maximum likelihood function in case of Gaussian mixture distribution. *Australian Journal of Earth Sciences* **63**, pp. 237 - 256 (2016).

[3] J. AWANGE, B. PALÁNCZ, R. LEWIS, L. VOLGYESI, *Mathematical Geosciences: Hybrid Symbolic-Numeric Methods*. Springer International Publishing AG, New York, 2018.

[1]Department of Mathematics
Fordham University
New York, USA
rlewis@fordham.edu

[2]Department of Photogrammetry and Geoinformatics
Budapest University of Technology and Economics
Budapest, Hungary
palancz.bela@epito.bme.hu

[3]Department of Spatial Sciences
Curtin University
Perth, Australia
J.Awange@curtin.edu.au

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Resultants, Implicit Parameterizations, and Intersections of Surfaces

Robert H. Lewis[1],

A classic problem in computer graphics and computer aided design is to derive an implicit equation for a surface given a parameterization of it. Since our surfaces are in three-dimensional space, we conventionally have three equations

$$\begin{aligned} x &= f(s,t) \\ y &= g(s,t) \\ z &= h(s,t) \end{aligned}$$

If homogeneous coordinates are being used, there is a fourth equation for w.

The implicit equation is produced by eliminating the s and t. As a very simple two-dimensional example, for a circle of radius r, the parametric equations are $x = r\cos(\theta), y = r\sin(\theta)$. It is easy to eliminate θ by squaring and adding:

$$x^2 + y^2 = r^2\cos^2(\theta) + r^2\sin^2(\theta) = r^2$$

yielding the familiar equation for a circle. (r is not a variable, but a *parameter* in the other sense of the word "parameter.") Real examples of interest are much more complicated than this, and sophisticated elimination techniques are needed.

The simple example illustrates an important idea. Parametric systems frequently involve trig functions, usually sine and cosine. Elimination techniques usually require polynomial (or rational) functions. A system with sine and cosine is easily converted to a polynomial system by replacing cosine with, say, ct, sine with st, and adding a new equation $ct^2 + st^2 - 1 = 0$.

The theory of eliminating variables from a system of equations has a long history, starting with Bezout around 1760. A key idea is the *resultant* of a system of polynomial equations [2], [8]. Bezout did this for one-variable polynomials. Dixon in 1908 extended it to multivariate polynomials, and proved it would work in a certain ideal situation. However, for real problems the ideal situation rarely applies and often the method seems to fail. Kapur, Saxena, and Yang showed how to get around all those problems in 1994 [3]. Lewis refined and greatly improved the method in 2008 [4] to what is called Dixon-EDF. Gröbner bases can also be used to eliminate variables [8].

In spite of the 1994 publication, the Kapur-Saxena-Yang (KSY) method seems to have not been noticed by the computer graphics community. In 2000 the authors of [1] explicitly reject resultants as unworkable. In 2004 Wang [9] was aware of

the Bezout-Dixon method but not KSY. He develops a new method to implicitize surfaces and tests fifteen examples with his method, resultants, and Gröbner bases. As in [1] he reports that in many cases resultants will not work because the Dixon method returns 0. This is one of the situations that KSY overcomes!

We compare Wang's reported time using pre-KSY Dixon, Wang's method, and our solution today using Dixon-KSY-EDF. We find our method to be greatly superior.

In 2017 Shen and Goldman [6] also report a new method for certain implicitizations. They also say that some resultant matrices have a 0 determinant and therefore resultants cannot be used. They do not refer to KSY.

We compare their reported times and our solutions today using Dixon-EDF working on some of their examples.

They try resultants in the generalized Sylvester form as found in [7] on their examples, and they also try Gröbner basis techniques. Gröbner bases failed in every case, meaning that nothing was returned within 10 minutes. Their resultants failed in the same way in every case except example 10.

Out techniques always work, are more efficient, and are more general.

In the following, Dixon always denotes the complete combination Dixon-KSY-EDF.

A second very important problem is to compute the intersection of two surfaces. Many papers have addressed this question. Virtually all the papers assume that the surfaces are *quadric*, i.e., degree 2. This means that the implicit equation is of the form

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz + gx + hy + iz + j = 0$$

We describe here an apparently new way to compute intersections so long as at least one of the surfaces is given by a conventional parameterization, as in the previous section. There is no restriction on the degrees of the surfaces, at least theoretically. Suppose surface one is given by

$$x = f_1(s_1, t_1), \;\; y = g_1(s_1, t_1), \;\; z = h_1(s_1, t_1)$$

and surface two is

$$x = f_2(s_2, t_2), \;\; y = g_2(s_2, t_2), \;\; z = h_2(s_2, t_2)$$

For the intersection simply combine this to form a system of six equations. Use Dixon to eliminate five variables, say y, z, t_1, s_2, t_2. That yields one equation (resultant) involving x and s_1. If this is linear in x, solve for x and obtain the parametric equation for the x-coordinate of the intersection curve. Repeat for y and z. One could just as well express x in terms of s_2, t_1 or t_2. That might have computational advantages.

The process described above also works if one surface has a parameterization and the second has an implicit definition, say $p(x, y, z) = 0$. We then have four equations $x = f_1(s_1, t_1), y = g_1(s_1, t_1), z = h_1(s_1, t_1), p(x, y, z) = 0$ and we eliminate three variables, say y, z, t_1.

If the resultant is degree 2 in x, one can easily use the quadratic formula to get two possible expressions for x in terms of s_1. Numerical testing could determine which is correct. Of course, degree 3 or 4 could also be handled by formulas, but the expressions would no doubt become daunting.

What if the degrees are higher than 2 or we don't want to deal with messy formulas? This leads to a new concept:

Definition: An implicit parameterization of a curve in 3-space is a set of three equations

$$f(x,s) = 0, \;\; g(y,s) = 0, \;\; h(z,s) = 0$$

whose solution set includes the curve. s is called the curve parameter.

Theorem Given two surfaces defined as above with polynomial functions, the Dixon resultant will produce an implicit parameterization of their intersection.

This follows immediately from the above discussion. The only possible flaw is if the set of six (or four) equations does not have a zero-dimensional solution space. That means for some values of the parameter s_1 there are infinitely many values of x. Dixon can fail in that case.

We will illustrate our techniques with many examples.

In summary,

- Computing an implicitization with Dixon is straightforward and routine. No special conditions on the surfaces are needed.
- The concept introduced here of "implicit parameterization" is easy to compute with Dixon. No special conditions on the surfaces are needed.
- Implicit parameterizations can be dealt with in fairly straightforward ways with commercial software.

Keywords: surface, polynomial system, resultant, Dixon, parameters, intersection, Gröbner basis

References

[1] Cox, D., Goldman R., Zhang M. On the validity of implicitization by moving quadrics for rational surfaces with no base points. Journal of Symbolic Computation 29 (3), pp. 419-440 (2000).

[2] Cox D., Little J., O'Shea D,. Using Algebraic Geometry. Graduate Texts in Mathematics, 185. Springer-Verlag. New York, 1998.

[3] Kapur D., T. Saxena T., and Yang L., Algebraic and geometric reasoning using Dixon resultants. In: *Proc. of the International Symposium on Symbolic and Algebraic Computation.* A.C.M. Press (1994).

[4] Lewis R. H., Heuristics to accelerate the Dixon resultant, Mathematics and Computers in Simulation 77 (4) pp. 400 - 407 (2008).

[5] Lewis R. H., Fermat code for Dixon-EDF, http://home.bway.net/lewis/dixon

[6] Shen L, Goldman R., Implicitizing Rational Tensor Product Surfaces Using the Resultant of Three Moving Planes. ACM Transactions on Graphics 36 (5), pp. 1-14 (2017).

[7] Shi X., Wang X., Goldman R. Using μ-bases to implicitize rational surfaces with a pair of orthogonal directrices. Computer Aided Geometric Design 29 (7), pp. 541-554 (2012).

[8] Sturmfels B., Solving systems of polynomial equations. CBMS Regional Conference Series in Mathematics 97, American Mathematical Society (2003).

[9] Wang, D., A simple method for implicitizing rational curves and surfaces. Journal of Symbolic Computation 38 pp. 899-914 (2004).

[1]Department of Mathematics
Fordham University
New York, USA
rlewis@fordham.edu

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Presentation of "The Gröbner Cover"

Antonio Montes[1]

I present the book "*The Gröbner Cover*" [6], that will be published during the present year. The contents are the following:

The genesis of this book is paper [7] for studying parametric polynomial systems.

Part 1 Theory: contains all the necessary tools to prove the existence and computation methods for obtaining the Canonical Gröbner Cover of a parametric polynomial system; Particularly, in Chapter 3, we provide the definitions and computation methods for obtaining all the canonical representations of constructible sets [3] and locally closed sets, that are used in Chapter 5 to obtain the Gröbner Cover, as well as for defining and computing all the algorithms provided in Part 2.

Part 2 Applications: contains three natural and interesting applications. Chapter 6 develops a new algorithm for Automatic Deduction of Geometric Theorems (`ADGT`) that, given a common geometric proposition of the form $(H \wedge \neg H_1) \Rightarrow (T \wedge \neg T_1)$, determines complementary hypothesis for the proposition to become a Theorem. The approach to this application was initiated in [5], but the new algorithm has not yet been published. Concerning Chapter 7, we introduced in [1] the taxonomy of the irreducible components of a Geometric Locus, which is determined by our `locus` algorithm. The content of Chapter 8, which has not yet been published either, generalizes the classical definitions, theorems and algorithms [2] for determining the

envelope of a family of hyper-surfaces with more degrees of freedom than usual. Moreover, a new algorithm for determining the irreducible algebraic components of the envelope, as well as two other algorithms for approaching the real projection of the envelope are provided.

All the algorithms described in the text are implemented in the Singular library “grobcov.lib" [8], whose latest implementation can be downloaded from the web [4]. The book can also be used as a User Manual for the library.

In the talk I will present some examples using the new algorithms to show their utility and I will give a general outlook about the book.

Keywords: Parametric Polynomial System, Canonical Discussion, Parametric Gröbner System, Gröbner System.

References

[1] M. A. ABANADES; F. BOTANA; A. MONTES; T. RECIO, An Algebraic Taxonomy for Locus Computation in Dynamic Geometry, *Computer Aided Geometrical Design*, **56**, 22-33, (2014).

[2] F. BOTANA; T. RECIO, Computing envelopes in dynamic geometry environments, *Annals of Mathematics and Artificial Intelligence*, 1-18, (2016).

[3] J. M. BRUNAT; A. MONTES, Computing the Canonical Representation of Constructible Sets, *International Journal of Mathematics in Computer Science*, **10**, 165–178, (2016).

[4] A. MONTES, `http://www-ma2.upc.edu//en/people/antonio.montes/`, Updated on (2018).

[5] A. MONTES; T. RECIO, Generalizing the Steiner-Lehmus theorem using the Gröbner cover, *Mathematics and Computers in Simulation*, **104**, 67-81, (2014).

[6] A. MONTES, *The Gröbner Cover*, ACM series, Springer, Berlin, Heidelberg, New York (2018).

[7] A. MONTES; M. WIBMER, Gröbner bases for polynomial systems with parameters, *Journal of Symbolic Computation*, **45**, 1391–1425, (2010).

[8] A. MONTES; H. SCHÖNEMANN, Singular “grobcov.lib" library 4-1-1, `http://www.singular.uni-kl.de`, Computer Algebra System for polynomial computations. Center for Computer Algebra, University of Kaiserslautern, free software under the GNU General Public Licence, (2018).

[1]Dep. Matemàtica Aplicada
Universitat Politècnica de Catalunya
Campus Nord, 08034-Barcelona, Spain
antonio.montes@upc.edu

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Computation methods of b-functions associated with μ-constant deformations – Case of inner modality 2 –

Katsusuke Nabeshima[1], **Shinichi Tajima**[2]

In this talk, computation methods of parametric b-functions are introduced for μ-constant deformation of quasihomogeneous singularities. The methods of b-functions associated with μ-constant deformations are constructed by using comprehensive Gröbner systems and the set of candidates of roots. In the cases of iner modality 2 ([7]), all b-funtions of associated with μ-constant deformations, can be obtained by our computation methods.

Let $\mathbb{C}\langle x, \partial_x\rangle$ denote the Weyl algebra, the ring of linear partial differential operators with coefficients in $\mathbb{C}$, where $x = (x_1, \ldots, x_n)$, $\partial_x = (\partial_1, \ldots, \partial_n)$, $\partial_i = \frac{\partial}{\partial x_i}$.

Let f be a non-constant polynomial in $\mathbb{C}[x]$. Then, the annihilating ideal of f^s is $\mathrm{Ann}(f^s) := \{p \in \mathbb{C}\langle s, x, \partial_x\rangle | pf^s = 0\}$ where s is an indeterminate. The *b-function* or the *Bernstein-Sato polynomial* of f is defined as the monic generator $b_f(s)$ of $(\mathrm{Ann}(f^s) + \mathrm{Id}(f)) \cap \mathbb{C}[s]$ where $\mathrm{Id}(f)$ is the ideal generated by f. It is known that the b-function of f always has $s+1$ as a factor and has a form $(s+1)\tilde{b}_f(s)$, where $\tilde{b}_f(s) \in \mathbb{C}[s]$. The polynomial $\tilde{b}_f(s)$ is called the *reduced b-function* of f.

It is known that a basis of the ideal $\mathrm{Ann}(f^s)$ can be computed by utilizing a Gröbner basis in $\mathbb{C}\langle x, \partial_x\rangle$ or PWB algebra ([5]). Moreorver, the reduced b-function $\tilde{b}_f(s)$ can be obtained by computing a Gröbner basis of $\mathrm{Ann}(f^s) + \mathrm{Id}(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n})$.

Let f be a parametric polynomial in $(\mathbb{C}[u])[x]$ where $u = (u_1, \ldots, u_m)$ and u are parameters. In our previous paper [4], a computation method of comprehensive Gröbner systems (CGS) has been introduced in Poincare-Birkhoff-Witt (PBW) algebras. Thus, theoretically, a CGS of the ideal $\mathrm{Ann}(f^s)$ can be computed by utilizing the computation method. Moreover, a CGS of the ideal $\mathrm{Ann}(f^s) + \mathrm{Id}(f)$ can be computed, too. Hence, parametric b-functions can be computed by the following algorithm.

Algorithm 1.

Input: f: a parametric polynomial.
Output: reducded b-functions of f.
STEP 1: Compute a CGS of $\mathrm{Ann}(f^s)$.
STEP 2: Compute a CGS of $\mathrm{Ann}(f^s) + \mathrm{Id}(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n})$.

Algorithm 1 has been implemented in the computer algebra system Risa/Asir.

Table 1: reduced b-functions of $x^2z + yz^2 + y^6 + u_1y^4z + u_2z^3$

strata	reduced b-function
$\mathbb{C}^2\backslash\mathbb{V}(u_1)$	$B(s)(s+\frac{9}{8})(s+\frac{23}{24})$
$\mathbb{V}(u_1)\backslash\mathbb{V}(u_1,u_2)$	$B(s)(s+\frac{9}{8})(s+\frac{47}{24})$
$\mathbb{V}(u_1,u_2)$	$B(s)(s+\frac{17}{8})(s+\frac{47}{24})$

The Milnor number μ of the singularity $x^2z+yz^2+y^6=0$ is 17 (S_{17} singularity, the inner modality is 2), and the μ-constant deformation is given by $f = x^2z+yz^2+y^6+u_1y^4z+u_2z^3$ where u_1, u_2 are parameters. Our implementation can output Table 1 as the parametric reduced b-function of f within 5 hours where

$$B(s) = (s+\tfrac{3}{2})(s+\tfrac{4}{3})(s+\tfrac{7}{6})(s+\tfrac{11}{6})(s+\tfrac{7}{8})(s+\tfrac{11}{8})(s+\tfrac{13}{8})$$
$$\times(s+\tfrac{25}{24})(s+\tfrac{29}{24})(s+\tfrac{31}{24})(s+\tfrac{35}{24})(s+\tfrac{37}{24})(s+\tfrac{41}{24})(s+\tfrac{43}{24}).$$

Let us consider another example. The Milnor number of μ of the singularity $x^2z + yz^2 + xy^4 = 0$ is 16 (S_{16} singularity, the inner modality is 2), and the μ-constant deformation is given by $f = x^2z + yz^2 + xy^4 + u_1y^6 + u_2z^3$ where u_1, u_2 are parameters. In this case, our implementation of Algorithm 1 cannot return the parametric reduced b-function of f within "2 months". However, the implementation returns a CGS of $\mathrm{Ann}(f^s)$ within 1 day. Thus, we can infer that the computational complexity of $\mathrm{Ann}(f^s) + \mathrm{Id}(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n})$ is quite big.

In order to avoid the big computation, Levandovskyy and Martin-Morales [3] have introduced a smart idea. We adopt the idea for computing b-functions of μ-constant deformations. However, the idea is not good enough to decide b-functions of μ-constant deformations. We need a further computation step that is checking local cohomology solutions of each holonomic D-module associted with a root of $\tilde{b}(s) = 0$, to compute b-functions of μ-constant deformations.

In this talk, we introduce the further computation step and the new algorithm for computing b-functions associated with μ-constant deformations.

Let $f(u,x) = f_0 + g \in (\mathbb{C}[u])[x]$ be a semi-quasihomogeneous polynomial, where f_0 is the quasihomogeneous part (or weighted homogeneous part) and g is a linear combination of upper monomials with parameters u. Then, f can be regard as a μ-constant deformation of f_0 with an isolated singularity at the origin. We have the foolowing classical results.

Theorem 1 Let $E_{f_0} = \{\gamma \in \mathbb{Q} | \tilde{b}_{f_0}(\gamma) = 0\}$ where $\tilde{b}_{f_0}$ is the reduced b-function of f_0 on the origin. Then, for $e \in \mathbb{C}^m$, the set of roots of b-function of $f(e,x)$, on the origin, the set $E_{f(e,x)} = \{\gamma | b_{f(e,x)}(\gamma) = 0\}$ becomes a subset of $E = \{\gamma - \ell \in \mathbb{Q} | \gamma \in E_{f_0}, \ell \in \mathbb{Z}, -n < \gamma - \ell < 0\}$ where $\mathbb{Z}$ is the set of integers. That is, $E_{f(e,x)} \subset E$, for $e \in \mathbb{C}^m$.

Theorem 2 Let f be a non-constant polynomial in $\mathbb{C}[x]$, H a basis of $\mathrm{Ann}(f^s)$ in $\mathbb{C}\langle s, x, \partial_x\rangle$, $\gamma \in \mathbb{Q}$ and $r \in \mathbb{N}$. Let G be a minimal Gröbner basis of $\mathrm{Id}(H \cup$

$\{f, \frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \ldots, \frac{\partial f}{\partial x_n}\} \cup \{(s-\gamma)^r\})$ w.r.t. a block term order $\succ$ s.t. $x \cup \partial_x \gg s$. Then, if $(s-\gamma)^r \in G$, $(s-\gamma)^r$ is a factor of the b-function of f.

The outline of the new algorithm is the following.

Algorithm 2.

Input: f: a parametric polynomial.
Output: reducded b-functions of f.
STEP 1: Compute a set E of candidates of roots of $\tilde{b}_f(s) = 0$.
STEP 2: Compute a CGS of $\mathrm{Ann}(f^s)$.
STEP 3: Compute a minimal Gröbner basis G of $\mathrm{Ann}(f^s) + \mathrm{Id}((s-\gamma)^r, f)$ (or $\mathrm{Id}((s-\gamma)^r$,
$f, \frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \ldots, \frac{\partial f}{\partial x_n})$) in $\mathrm{C}[s]\langle x, \partial_x\rangle$ where $\gamma \in E$ and $r \in \mathrm{N}_{>0}$.
If $(s-\gamma)^r \in G$, then $(s-\gamma)^r$ is a factor of the b-function of f.
STEP 4: For each stratum, check local cohomology solutions of each holonomic D-module associated with the root of $\tilde{b}_f(s) = 0$.

By executing Algorithm 2, we can obtain Table 2 as the parametric reduced b-function of $f = x^2z + yz^2 + xy^4 + u_1y^6 + u_2z^3$ within 4 hours where

$$B(s) = (s+\tfrac{15}{17})(s+\tfrac{18}{17})(s+\tfrac{20}{17})(s+\tfrac{21}{17})(s+\tfrac{22}{17})(s+\tfrac{23}{17})(s+\tfrac{24}{17})(s+\tfrac{25}{17}) \times(s+\tfrac{26}{17})(s+\tfrac{27}{17})(s+\tfrac{28}{17})(s+\tfrac{29}{17})(s+\tfrac{30}{17})(s+\tfrac{31}{17}).$$

Table 2: reduced b-functions of $x^2z + yz^2 + xy^4 + u_1y^6 + u_2z^3$

strata	reduced b-function
$\mathbb{C}^2\backslash\mathbb{V}(u_1)$	$B(s)(s+\frac{16}{17})(s+\frac{19}{17})$
$\mathbb{V}(u_1)\backslash\mathbb{V}(u_1,u_2)$	$B(s)(s+\frac{19}{17})(s+\frac{33}{17})$
$\mathbb{V}(u_1,u_2)$	$B(s)(s+\frac{33}{17})(s+\frac{36}{17})$

In this talk, we present mainly Algorithm 2 and show all b-functions of μ-constant deformation of inner modality 2.

Keywords: b-functions, comprehensive Gröbner systems, local cohomology

References

[1] M. KATO, The b-function of μ-constant deformation of $x^7 + y^5$. *Bull. College of Science, Univ. of the Ryukyus* **32**, 5–10 (1981).

[2] K. NABESHIMA; S. TAJIMA, Algebraic local cohomology with parameters and parametric standard bases for zero-dimensional ideals. *J. Symbolic Computation* **82**, 91–122, (2017).

[3] V. LEVANDOVSKYY; V. MARTÍN-MORALES, Algorithms for checking rational roots of b-functions and their applications. *J. Algebra*, **352**, 408–429, (2012).

[4] K. NABESHIMA; K. OHARA; S. TAJIMA, Comprehensive Gröbner systems in PBW algebras, Bernstein-Sato ideals and holonomic $\mathcal{D}$-modules. *Journal of Symbolic Computation* in Press (2018).

[5] T. OAKU, An algorithm of computing b-functions. *Duku Math. J.* **87**, 115–132, (1997).

[6] T. YANO, On the theory of b-functions. *Publications of the Research Institute for Mathematical Sciences, Kyoto Univ.*, **14**, 111–202, (1978).

[7] E. YOSHINAGA; M. SUZUKI, Normal forms of nondegenerate quasihomogeneous functions with inner modality ≤ 4. *Invent. Math.*, **55**, 185–206, (1979).

[1]Graduate School of Technology, Industrial and Social Sciences,
Tokushima University,
2-1, Minamijosanjima, Tokushima, JAPAN
nabeshima@tokushima-u.ac.jp

[2]Graduate School of Pure and Applied Sciences,
University of Tsukuba,
1-1-1, Tennoudai, Tsukuba, JAPAN
tajima@math.tsukuba.ac.jp

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

An algorithm for computing Grothendieck local residues II — general case —

Katsuyoshi Ohara[1], **Shinichi Tajima**[2]

We will give an algorithm for exactly evaluating Grothendieck local residues for rational n-forms of n variables under general condition and show an implementation on a computer algebra system Risa/Asir. Grothendieck local residue is a natural generalization of the well-known residue for complex functions of single variable. The local residue was firstly described in Hartshorne [3] via the local duality in terms of derived category in much greater generality. The local duality can be also interpreted as a perfect pairing in terms of homological algebra. When a point is fixed, it can be realized as an integration of a meromorphic n-form of complex n variables on a real n-cycle around the point. Griffiths-Harris [2] described the following analytic definition of Grothendieck local residues.

Definition. Denote by $\mathcal{O}(U)$ a ring of holomorphic functions on a ball $U \subset \mathbf{C}^n$. Suppose that $f_1(x), \ldots, f_n(x) \in \mathcal{O}(U)$ 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 $\varphi(x) \in \mathcal{O}(U)$, 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 $\varphi(x)\tau_F$.

The integration certainly gives an explicit representation of the local residue at the point β. However, in general, it is very hard to directly evaluate the integration because of complicated geometric shape of the real n-cycle in the $2n$-dimensional real space. To solve this problem, we use a method based on D-modules.

Let K be a subfield of $\mathbf{C}$ and denote $K[x] = K[x_1, \ldots, x_n]$. We suppose that a polynomial sequence $F = \{f_1, \ldots, f_n\}$ with K-coefficients is regular. The polynomial ideal I generated by F is zero-dimensional. The zero set $V_{\mathbf{C}}(I) = \{a \in \mathbf{C}^n \mid g(a) = 0,\ \forall g \in I\}$ is finite and it consists of isolated common zeros of the regular sequence F.

We introduce the n-th *algebraic local cohomology group* with support on $Z = V_{\mathbf{C}}(I)$ by

$$H^n_{[Z]}(K[x]) = \lim_{k\to\infty} \mathrm{Ext}^n_{K[x]}(K[x]/(\sqrt{I})^k, K[x]).$$

The algebraic local cohomology group $H^n_{[Z]}(K[x])$ can be regarded as a collection of equivalent classes of rational functions whose denominator has zero only on Z. Here the equivalence is given by cutting holomorphic parts of rational functions in a cohomlogical way.

According to the primary decomposition $I = \bigcap_{\lambda=1}^{\ell} I_\lambda$, the zero set also can be written as union of irreducible affine varieties: $Z = \bigcup_{\lambda=1}^{\ell} Z_\lambda$, where $Z_\lambda = V_{\mathbf{C}}(\sqrt{I_\lambda})$. Then $H^n_{[Z]}(K[x])$ is decomposed to direct sum

$$H^n_{[Z]}(K[x]) = H^n_{[Z_1]}(K[x]) \oplus \cdots \oplus H^n_{[Z_\lambda]}(K[x]) \oplus \cdots \oplus H^n_{[Z_\ell]}(K[x]).$$

Therefore an algebraic local cohomology class $\sigma_F = \left[\frac{1}{f_1 \cdots f_n}\right] \in H^n_{[Z]}(K[x])$ has unique decomposition

$$\sigma_F = \sigma_{F,1} + \cdots + \sigma_{F,\lambda} + \cdots + \sigma_{F,\ell},$$

where $\sigma_{F,\lambda} \in H^n_{[Z_\lambda]}(K[x])$. Note that $\mathrm{supp}\,(\sigma_{F,\lambda}) \subset Z_\lambda$. The decomposition above is a kind of partial fractional expansion of $\frac{1}{f_1 \cdots f_n}$ in terms of local cohomology.

Let $\beta \in Z_\lambda$ and $\varphi(x) \in \mathcal{O}(U)$ where U is a small neighborhood of β. We want to evaluate the local residue $\mathrm{Res}_\beta(\varphi\tau_F)$ where $\tau_F = (f_1(x) \cdots f_n(x))^{-1} dx$ and $dx = dx_1 \wedge \cdots \wedge dx_n$. If $j \neq \lambda$, then each $\sigma_{F,j}$ vanishes on U because $\mathrm{supp}\,(\sigma_{F,j}) \cap U = \emptyset$. Thus $\mathrm{Res}_\beta(\varphi\tau_F) = \mathrm{Res}_\beta(\varphi\,\sigma_{F,\lambda} dx)$ for $\beta \in Z_\lambda$. We denote by δ_{Z_λ} the local cohomology class which represents the delta function with the support Z_λ.

The algebraic local cohomology group can be naturally endowed with a structure of D-module. On the support Z_λ, from general theory, it follows $H^n_{[Z_\lambda]}(K[x]) = D_n \delta_{Z_\lambda}$. In other words, there exists a linear differential operator $T_{F,\lambda} \in D_n$ such that $\sigma_{F,\lambda} = T^*_{F,\lambda} \bullet \delta_{Z_\lambda}$ where $T^*_{F,\lambda}$ stands for the formal adjoint of $T_{F,\lambda}$. Since the local residue can be described in terms of local cohomology, we have $\mathrm{Res}_\beta(\varphi\tau_F) = \mathrm{Res}_\beta(\left[\frac{\varphi dx}{f_1 \cdots f_n}\right])$. Therefore

$$\begin{aligned}
\mathrm{Res}_\beta(\left[\frac{\varphi dx}{f_1 \cdots f_n}\right]) &= \mathrm{Res}_\beta(\varphi\sigma_F dx) \\
&= \mathrm{Res}_\beta(\varphi \cdot (T^*_{F,\lambda} \bullet \delta_{Z_\lambda}) dx) \\
&= \mathrm{Res}_\beta((T_{F,\lambda} \bullet \varphi) \cdot \delta_{Z_\lambda} dx) \\
&= (T_{F,\lambda} \bullet \varphi)|_{x=\beta}.
\end{aligned}$$

That is, the mapping $\varphi \mapsto \mathrm{Res}_\beta(\varphi\tau_F)$ is determined by the differential operator $T_{F,\lambda}$. Since the set $\{(T_{F,\lambda}, Z_\lambda) \mid \lambda = 1, 2, \ldots, \ell\}$ gives the Grothendieck local residue mapping, the local residue of any meromorphic n-forms can be evaluated by differential operators $T_{F,\lambda}$. Our purpose is to find the differential operator $T_{F,\lambda}$ without the use of an explicit representative element of the local cohomology class $\sigma_{F,\lambda}$.

Under certain condition for the regular sequence F, we already gave an algorithm for computing differential operators $T_{F,\lambda}$ (see [6]). We have extended the method

for more general setting. In this talk, we will describe new algorithm and show an implementation on the computer algebra system. Our algorithm consists of the following steps.

1. Find the primary decomposition $I = \bigcap_{\lambda=1}^{\ell} I_\lambda$.
2. Find the annihilating left-ideal $\mathrm{Ann}_{D_n}(\sigma_F)$.
3. For each λ, find the vector space V_λ over $K[x]/\sqrt{I_\lambda}$ spanned by Noether differential operators of the associated prime $\sqrt{I_\lambda}$.
4. For each λ, find a "monic" operator $S_\lambda^* \in V_\lambda$ such that $\mathrm{Ann}_{D_n}(\sigma_F) S_\lambda^* \subset \mathrm{Ann}_{D_n}(\delta_{F,\lambda})$.
5. For each λ, determine the differential operator $T_{F,\lambda}^*$ from S_λ^*.

Keywords: Local residues, Local Cohomology, Holonomic System

References

[1] A. Altman and S. Kleiman, *Introduction to Grothendieck Duality Theory*, Lecture Notes in Mathematics **146**, Springer, 1970.

[2] P. Griffiths and J. Harris, *Principles of Algebraic Geometry*, Wiley Interscience, 1978.

[3] R. Hartshorne, *Residues and Duality*, Lecture Notes in Mathematics **20**, Springer, 1966.

[4] L. Hörmander, *An Introduction to Complex Analysis in Several Variables*, the third revised edition, North-Holland, 1990.

[5] Y. Nakamura and S. Tajima, Residue calculus with differential operator, Kyushu Journal of Mathematics **54** (2000), 127–138.

[6] K. Ohara and S. Tajima, An algorithm for computing Grothendieck local residues I — shape base case — , *Abstracts of 23rd Conference on Applications of Computer Algebra — ACA 2017*, 226–227, 2017.

[7] 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.

[8] S. Tajima, Noether differential operators and Grothendieck local residues, RIMS Kôkyûroku **1432** (2005), 123–136. (in Japanese)

[9] S. Tajima and Y. Nakamura, Computational aspects of Grothendieck local residues, Séminaires et Congrès **10** (2005), 287–305.

[1]Faculty of Mathematics and Physics
Kanazawa University, Japan.
Kakuma-machi Kanazawa, 920-1165, Japan
ohara@se.kanazawa-u.ac.jp

[2]Institute of Mathematics
University of Tsukuba
1-1-1 Tennodai, Tsukuba 305-8571, Japan
tajima@math.tsukuba.ac.jp

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

A canonical representation of continuity of the roots of a parametric zero dimensional multi-variate polynomial ideal

Yosuke Sato[1], **Ryoya Fukasaku**[2], **Hiroshi Sekigawa**[3]

In [2, 3], we introduced the following result **Theorem 1** which gives a sufficient condition of a generator of a multivariate parametric zero dimensional ideal for the continuity property of its roots. In [3], using the result we also give a correctness proof of an algorithm for real quantifier elimination one of the authors has recently developed and implemented in [1]. In this talk, using the theory introduced in [4], we show the following results **Theorem 2** and **Theorem 3** which enable us both to describe and to compute a canonical representation form of continuity of the roots of a given parametric zero dimensional multi-variate polynomial ideal.

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 $\mathbb{Q}[\bar{A}, \bar{X}]$.*
2. *$\{\mathcal{S}_1, \ldots, \mathcal{S}_k\}$ is an algebraic partition of S.*

3. *For each $\bar{c} \in \mathcal{S}_i$, $G_i(\bar{c}) = \{g(\bar{c}, \bar{X}) | g(\bar{A}, \bar{X}) \in G_i\}$ is a Gröbner basis of the ideal $\langle F(\bar{c})\rangle$ in $\mathbb{C}[\bar{X}]$ w.r.t. $\succ$, where $F(\bar{c}) = \{f(\bar{c}, \bar{X}) | f(\bar{A}, \bar{X}) \in F\}$.*

4. *For each $\bar{c} \in \mathcal{S}_i$, $LC(g)(\bar{c}) \neq 0$ for any element g of G_i.*

In addition, if each $G_i(\bar{c})$ 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.

The following fact is one of the most important properties of a minimal comprehensive Gröbner system.

Fact 1. $LT(G_i(\bar{c}, \bar{X}))$ is identical for each $\bar{c} \in \mathcal{S}_i$. Hence, the dimension of a $\mathbb{C}$-vector space $\mathbb{C}[\bar{X}]/\langle G_i(\bar{c}, \bar{X})\rangle$ is invariant for $\bar{c} \in S_i$ if it is finite. Consequently, when the $\mathbb{C}$-vector space has dimension l for each $\bar{c} \in S_i$, the ideal $\langle G_i(\bar{c}, \bar{X})\rangle$ has l number of roots in $\mathbb{C}^n$ counting their multiplicities.

Considering the above roots as a l size multiset and introducing a natural topology on a set of the same size multisets, we have the following property.

Theorem. *Let $\mathcal{G} = \{(\mathcal{S}_1, G_1), \ldots, (\mathcal{S}_k, G_k)\} \subset \mathbb{Q}[\bar{X}, \bar{A}]$ be a minimal comprehensive Gröbner system with parameters $\bar{A}$ w.r.t. an arbitrary term order of main variables $\bar{X}$. If the ideal $\langle G_i(\bar{c})\rangle$ is zero dimensional for each $\bar{c} \in \mathcal{S}_i$, then the set of all roots of the system of the parametric polynomial equations $g(\bar{A}, \bar{X}) = 0, g \in G_i$ is continuous in the segment $\mathcal{S}_i$ as a function of the parameters $\bar{A}$.*

Note that the multisets of the roots of two ideals $\langle G_i(\bar{a})\rangle$ and $\langle G_j(\bar{b})\rangle$ for $\bar{a} \in \mathcal{S}_i$ and for $\bar{b} \in \mathcal{S}_j$ may have the same size for some different i, j, even when $LT(G_i(\bar{c}, \bar{X}))$ and $LT(G_j(\bar{c}, \bar{X}))$ are distinct. For such a case we still have the following property.

Theorem. *Using the same notations in the previous theorem, if the multisets of the roots of two ideals $\langle G_i(\bar{c})\rangle$ and $\langle G_j(\bar{c})\rangle$ have the same size but $LT(G_i(\bar{c}, \bar{X}))$ and $LT(G_j(\bar{c}, \bar{X}))$ are distinct, then two segments $\mathcal{S}_i$ and $\mathcal{S}_j$ are not path-connected.*

This property enables us to describe a canonical representation form of continuity of the roots of a given parametric multi-variate polynomial ideal as follows.

Theorem. *Given a finite set F of $\mathbb{Q}[\bar{A}, \bar{X}]$ and a term order $\succ$. There exists a unique partition $\{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_k\}$ of $\mathbb{C}^m$ such that the following properties hold.*

1. *Each $\mathcal{A}_i$ is an algebraically constructible set.*

2. *$LT(\langle F(\bar{c}, \bar{X})\rangle)$ is invariant for $\bar{c}$ on each $\mathcal{A}_i$.*

3. *$LT(\langle F(\bar{a}, \bar{X})\rangle)$ and $LT(\langle F(\bar{b}, \bar{X})\rangle)$ are distinct if $\bar{a} \in \mathcal{A}_i$ and $\bar{b} \in \mathcal{A}_j$ for different i, j.*

4. *If $\langle F(\bar{c}, \bar{X})\rangle$ has finite zeros in $\mathbb{C}^n$ for $\bar{c}$ on $\mathcal{A}_i$, the map from $\mathcal{A}_i$ to the set of multisets of such zeros is continuous.*

5. *If* $\mathbb{C}[\bar{X}]/\langle F(\bar{a},\bar{X})\rangle$ *and* $\mathbb{C}[\bar{X}]/\langle F(\bar{b},\bar{X})\rangle$ *have the same finite dimension as* $\mathbb{C}$ *vector space for* $\bar{a} \in \mathcal{A}_i$ *and* $\bar{b} \in \mathcal{A}_j$ $(i \neq j)$*, then* $\mathcal{A}_i$ *and* $\mathcal{A}_j$ *are not path-connected.*

Remark 1. Using the theory of [4], we can also compute such a partition $\{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_k\}$ from a given finite set F of $\mathbb{Q}[\bar{A}, \bar{X}]$.

Remark 2. The partition $\{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_k\}$ depends on the choice of a term order, however, it seems to be independent, though we have not shown it yet.

Keywords: Comprehensive Gröbner System, Representation of Continuity, Quantifier Elimination

References

[1] Fukasaku, R.: 2017 Version of **CGSQE** Package.
`http://www.rs.tus.ac.jp/fukasaku/software/CGSQE-2017/`.

[2] Sato, Y., Sekigawa, H.: On continuity of the roots of a parametric zero dimensional multivariate polynomial ideal, Book of Abstracts, 23rd Conference on Applications of Computer Algebra, pp.224-225, 2017.

[3] Sato, Y., Fukasaku, R., Sekigawa, H.: On continuity of the roots of a parametric zero dimensional multivariate polynomial ideal, to appear in Proceedings of ISSAC2018, 2018.

[4] Suzuki, A., Sato, Y.: An Alternative Approach to Comprehensive Gröbner Bases. JOURNAL OF SYMBOLIC COMPUTATION, Vol.36/3-4, pp.649-667, 2003.

[1]Department of Applied Mathematics,
Tokyo University of Science,
1-3,Kagurazaka,Shinjuku-ku, Tokyo, JAPAN
`ysato@rs.kagu.tus.ac.jp`

[2]Department of Applied Mathematics,
Tokyo University of Science,
1-3,Kagurazaka,Shinjuku-ku, Tokyo, JAPAN
`fukasaku@rs.tus.ac.jp`

[3]Department of Applied Mathematics,
Tokyo University of Science,
1-3,Kagurazaka,Shinjuku-ku, Tokyo, JAPAN
`sekigawa@rs.tus.ac.jp`

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

An effective method for computing Grothendieck point residues

Shinichi Tajima[1], **Katsusuke Nabeshim**[2]

In this talk, we present an effective algorithm for computing Grothendieck local residues associated to semi-quasi homogeneous hypersurface isolated singularities. The key idea of our approach is the use of Grothendieck local duality.

The theory of Grothendieck local residue is a cornerstone of algebraic geometry and complex analysis. It has been used in diverse problems of several different fields of mathematics. It is known theoretically that the classical transformation law given in [2] can be used to compute its values. Whereas computing Grothendieck local residue is quite difficult even if one uses computer algebra systems, because of the cost of computation in local rings. Developing effective methods for computing has been desired in many applications.

We consider in this talk Grothendieck point residues associated to a μ-constant deformation of quasi-homogeneous hypersurface isolated singularity. Based on the theory of local cohomology and Grothendieck local duality, we propose a new effective method for computing Grothendieck local residues. A key innovation of the resulting algorithm is an improvement of a previous algorithm on extended ideal membership problems in the ring of convergent power series [5].

To be more precise, let $f(x,t) = f_0(x) + g(x,t)$ be a semi-quasi homogeneous polynomial, where $f_0(x)$ is the quasi-homogeneous part, $g(x,t) = \sum_{j=1}^{\ell} t_j x^{\beta_j}$ is a sum of upper monomials with $x = (x_1, x_2, ..., x_n)$ main variables, $t = (t_1, t_2, ..., t_\ell)$ deformation parameters. Set $F = [\frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, ..., \frac{\partial f}{\partial x_n}]$ and let $\tau_F = [\ \frac{1}{\frac{\partial f}{\partial x_1} \cdot \frac{\partial f}{\partial x_2} \cdots \frac{\partial f}{\partial x_n}}\ ]$ denote the local cohomology class in $\mathcal{H}^n_{\{\mathcal{O}\}}(\mathcal{O}_X)$ with parameters t where $[\ \frac{1}{\frac{\partial f}{\partial x_1} \cdot \frac{\partial f}{\partial x_2} \cdots \frac{\partial f}{\partial x_n}}\ ]$ is the Grothendieck symbol.

Let $res_{\{\mathcal{O}\}}(h, \tau_F dx)$ denote the Grothendieck point residue at the origin $\mathcal{O}$ in $\mathbf{C}^n$ of the differential form

$$\frac{h(x)}{\frac{\partial f}{\partial x_1} \cdot \frac{\partial f}{\partial x_2} \cdots \frac{\partial f}{\partial x_n}} dx_1 \wedge dx_2 \wedge \cdots \wedge dx_n,$$

where $h(x)$ is a germ of holomorphic function. The linear map which assigns to each holomorphic function $h(x)$ the Grothendieck point residue

$$h(x) \longrightarrow res_{\{\mathcal{O}\}}(h, \tau_F dx)$$

can be expressed in terms of partial differential operators. Namely there exists a linear partial differential operator T, s.t.

$$(Th)(\mathcal{O}) = res_{\{\mathcal{O}\}}(h, \tau_F dx)$$

By using algorithm for computing algebraic local cohomology classes with parameters ([4]) , we introduce an effective method for computing the linear partial differential operator T. We also show the resulting algorithm for computing Grothendieck point residues associated to a μ-constant deformation of quasi homogeneous hypersurface isolated singularity.

We present some examples of computation.

Keywords: Grothendieck local residue, local cohomology, Grothendieck local duality

References

[1] A. ALTMAN AND S. KLEIMAN, *Introduction to Grothendieck Duality Theory* . Lecture Notes in Math. **146**, Springer, 1970.

[2] R. HARTSHORNE, *Residues and Duality*. Lecture Notes in Math. **20**, Springer, 1966.

[3] P. GRIFFITHS AND J. HARRIS, *Principles of Algebraic Geometry*. Wiley Classics Library, 1978.

[4] K. NABESHIMA AND S. TAJIMA, On efficient algorithms for computing parametric local cohomology classes associated with semi-quasihomogeneous singularities and standard bases, In *Proc. International Symposium on Symbolic and Algebraic Computation*, K. Nabeshima (eds.), 351-358, ACM 2014.

[5] 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**, 252–267 (2016).

[6] K. NABESHIMA AND S. TAJIMA, Algebraic local cohomology with parameters and parametric standard bases for zero-dimensional ideals. *J. Symb. Comput.* **82**, 91–122 (2017).

[7] S. TAJIMA AND Y. NAKAMURA, Annihilating ideals for an algebraic local cohomology class. *J. Symb. Comput.* **44**, 435–448 (2009).

[1]Graduate School of Pure and Applied Sciences,
University of Tsukuba,
1-1-1, Tennoudai, Tsukuba, JAPAN
tajima@math.tsukuba.ac.jp

[2]Graduate School of Technology, Industrial and Social Sciences,
Tokushima University,
2-1, Minamijosanjima, Tokushima, JAPAN
nabeshima@tokushima-u.ac.jp

S11
Algorithms for Zero-Dimensional Ideals

In the last decades, a lot of progress has been made on the study of efficient algorithms related to zero-dimensional ideals, including for solving polynomial systems, i.e. determining the finite set of roots common to a given collection of multivariate polynomials. During this process, it has turned out that these algorithms heavily rely on some routines from linear algebra. This session will focus on the design and the implementation of algorithms specifically tailored for the particular linear algebra problems encountered in this kind of computations. Applications of these techniques will also be considered, such as algebraic cryptanalysis and decoding algorithms for algebraic geometry codes.

Polynomial system solving often involves computing a first Groebner basis, typically with the F5 algorithm, and then working on finding a representation of the sought roots, using for example the FGLM algorithm. In the first step, one has to deal with matrices of large dimension which are sparse and exhibit a noticeable structure. The second step corresponds to finding the nullspace of a matrix with a multi-Krylov structure: the matrix is formed by some vector and its images by successive powers of the so-called multiplication matrices.

It has been observed that these multiplication matrices are most often sparse, a feature that one wants to exploit to obtain faster algorithms. So far, two approaches have been used to achieve this. One is inspired from the block Wiedemann algorithm, involving the computation of the generator for a linearly recurrent matrix sequence; the other one relies on the computation of generators for a multi-dimensional linearly recurrent sequence. This revived interest into the latter problem, with the goal of designing algorithms which outperform the Sakata algorithm, known for its applications to the decoding of algebraic geometry codes. Some approaches have already been described, involving computations with matrices that have a multi-layered block-Hankel structure.

This session aims at gathering the main actors behind the recent advances, and naturally all researchers interested in this topic and its future

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Border basis, Hilbert Scheme of points and flat deformations

Mariemi Alonso[1], **Jerome Brachat**[2], **Bernard Mourrain**[3]

A natural question when studying systems of polynomial equations is how to characterize the family of ideals which defines a fixed number μ of points counted with multiplicities. Understanding the allowed perturbations of a zero-dimensional algebra, which keep the number of solutions constant, is an actual challenge, in the quest for efficient and stable numerical polynomial solvers.

From a theoretical point of view, this question is related to the study of the Hilbert Scheme of μ points introduced by Grothendieck.

Many works were developed to analyze its geometric properties, (eg. Hartshorne (1965), [3] and many others). Though the Hilbert functor is known to be representable its effective representation is still under investigation. Using the persistence theorem of Gotzmann (1978), a global explicit description of the Hilbert scheme is given in [4] as a sub-scheme of a product of two Grassmannians. Equations defining $\mathrm{Hilb}^{\mu}(\mathbb{P}^n)$ in a single Grassmannian are also given in [4]. These equations, obtained from rank conditions in the vector space of polynomials in successive "degrees", have a high degree in the Plücker coordinates.

In the last years the problem of representation is also studied through sub-functor constructions and open covering of charts of the Hilbert scheme. Covering charts corresponding to subsets of ideals with a fixed initial ideal for a given term ordering. These ideas, starting with the proof of the irreducibility of Hartshorne (1965), and Bayer's PhD (1982)), were analyzed in several works, from the 80's; Carrá-Ferro (1988), Mark Haiman (1994), Huibregtse (2002), and more recent in [5] and [7].

These open subsets can be embedded into affine o pen s ubsets o f t he Hilbert scheme, corresponding to ideals associated to quotient algebras with a given monomial basis. Explicit equations of these affine varieties are developed for some special cases in the references above, and using syzygies or in more general setting in [5]. Their methods rely on simple algebraic construction and avoid the usual embeddings into high dimensional spaces. In this way, in [6] the authors obtain equations of low degree in a Grassmaniann for general Hilbert schemes.

In this talk, we concentrate in the punctual Hilbert scheme, and we show how to use Boorder basis to get new equations of it, of degree two in the Plucker coordinates of a Grassmaniann, which are simpler than Bayer and Iarrobino-Kanev equations [1]. Next, using Border basis we get an easy description of the tangent space at a point of $\mathrm{Hilb}^{\mu}(\mathbb{P}^n)$ [1]. We give also an effective criterion to test if a perturbed system

remains on the Hilbert scheme of the initial equations (test for a flat deformation), which involves a particular formal reduction with respect to border bases [2].

Finally, we introduce a "Newton Method" in the Hilbert scheme of points to find (numerically) a Border basis of a system of equations by using the knowledge of a border basis for some values of the coefficients nearby the ones of the given equations [2].

Keywords: Border basis, punctual Hilbert scheme, effective flat deformation of points

References

[1] MARIEMI ALONSO, JEROME BRACHAT, BERNARD MOURRAIN, The Hilbert Scheme of points and its link with border basis. *arXiv:0911.3503*, (2010).

[2] MARIEMI ALONSO, JEROME BRACHAT, BERNARD MOURRAIN, Flat Deformation of Points Communication in *MEGA2011*, Stockholm, May 30$^{\text{th}}$-June 3$^{\text{rd}}$, 2011.

[3] ANTHONY A. IARROBINO, Hilbert scheme of points: overview of last ten years. In *Algebraic geometry, Bowdoin, 1985 (Brunswick, Maine, 1985)*, vol. 46 of *Proc. Sympos. Pure Math.*, Amer. Math. Soc., Providence, RI, 1987.

[4] ANTHONY IARROBINO; VASSIL KANEV, In Appendix C of *Power sums, Gorenstein algebras, and determinantal loci*. vol. 1721 *Lecture Notes in Mathematics*, Springer-Verlag, Berlin, 1999.

[5] CRISTINA BERTONE, PAOLO LELLA, MARGHERITA ROGGERO, A Borel open cover of the Hilbert scheme, *J. Symb. Comput* **53** , 119–135 (2013).

[6] JEROME BRACHAT, PAOLO LELLA, BERNARD MOURRAIN, MARGHERITA ROGGERO, Extensors and the Hilbert scheme, *Annali della Scuola Normale Superiore di Pisa,Classe di Scienze,* **doi 10.2422/2036-2145.201407_003**, (2015).

[7] MATHIAS LEDERER, Groebner strata in the Hilbert scheme of points, *J. Commut. Algebra* **3**(3), 349–404 (2011).

[1]Departmento de Álgebra, Geometría y Topología
Complutense University
Plaza de Ciencias 3, 28040 Madrid (Spain)
mariemi@ucm.es

[3]Univ. Cote-d'Azur, Inria
Sophia-Antipolis, France
bernard.mourrain@inria.fr

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

On the decoding of interleaved and folded Reed-Solomon codes

Daniel Augot[1]

In 2006, great progress has been made in algebraic coding theory, where codes reaching the so-called list decoding capacity were constructed by Guruswami and Rudra [4], elaborating on the ideas of Parvaresh and Vardy [5]. At the heart of these constructions lies the simple notion of *folding* the codes, which is a very simple construction, at the cost of shortening the underlying Reed-Solomon codes and augmenting the size of the alphabet.

Later, Guruswami proposed another decoding method, call "linear algebraic" [3], which appears to be easier to deal with, from the computer algebra point of view.

Both these methods rely heavily on finite fields and their properties, a fact which is strange in this area, since the simple, classical, Guruswami-Sudan list decoding algorithm [1] works over any field, and all the arguments for proving its validity, studying its list size and decoding radius does not depend on the field. In other words, the Guruswami-Sudan list decoding algorithm can be said to be of "geometric" nature, while the decoding algorithms of folded Reed-Solomon have an "arithmetic" nature.

At the heart of the basic Guruswami-Sudan algorithm lies a bivariate interpolation problem, i.e. one has to find the vanishing ideal of a set of points given by the instance of decoding problem. Then it is followed by the so-called root-finding step: the codewords which are looked for correspond to components to a curve. Similarly, when generalizing to interleaved codes, the vanishing ideal of points in a higher dimensional space has to be computed. But in that case, the root-finding is ill-founded, and one should look for a zero dimensional ideal over the field of rational functions (or equivalently, a bivariate curve). This problem is circumvented using folding, and root-finding then involves a lot properties of finite fields.

In this talk, I will describe a potential path to new ideas for having a decoding algorithm of folded Reed-Solomon codes which does not assume the finiteness of the field, and may be more natural, with better list size. But first, for didactic purposes, I will recall the basic problems and settings posed by list decoding, recalling the "Shannon" versus "Hamming" opposed situations, and why list decoding bridges them [2].

References

[1] V. Guruswami and M. Sudan. On representations of algebraic-geometry codes. *Information Theory, IEEE Transactions on*, 47(4):1610–1613, 2001.

[2] Venkatesan Guruswami. List decoding of binary codes - a brief survey of some recent results. In Yeow M. Chee, Chao Li, San Ling, Huaxiong Wang, and Chaoping Xing, editors, *Coding and Cryptology*, volume 5557 of *Lecture Notes in Computer Science*, pages 97–106, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[3] Venkatesan Guruswami. Linear-algebraic list decoding of folded Reed-Solomon codes. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity, CCC 2011, San Jose, California, June 8-10, 2011*, pages 77–85, 2011.

[4] Venkatesan Guruswami and Atri Rudra. Explicit capacity-achieving list-decodable codes. In *STOC '06: Proceedings of the thirty-eighth annual ACM symposium on Theory of computing*, pages 1–10, New York, NY, USA, 2006. ACM.

[5] Farzad Parvaresh and Alexander Vardy. Correcting errors beyond the Guruswami-Sudan radius in polynomial time. In *FOCS 2005: Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science, Pittsburgh, United States*, pages 285–294, 2005.

[1]INRIA Saclay-Île-de-France, and École polytechnique
Palaiseau, France
daniel.augot@inria.fr

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Computing and Using Minimal Polynomials

John Abbott[1], **Anna M. Bigatti**[1], **Elisa Palezzato**[2], **Lorenzo Robbiano**[1]

Given a zero-dimensional ideal I in a polynomial ring, many computations start by finding univariate polynomials in I. Searching for a univariate polynomial in I is a particular case of considering the minimal polynomial of an element in P/I. It is well known that minimal polynomials may be computed via elimination, therefore this is considered to be a "resolved problem". But being the key of so many computations, it is worth investigating its meaning, its optimization, its applications.

If K is a field and R is a zero-dimensional affine K-algebra, *i.e.* a zero-dimensional algebra of type $R = K[x_1, \ldots, x_n]/I$, then R is a finite-dimensional K-vector space. Consequently, it is not surprising that minimal and characteristic polynomials can be successfully used to detect properties of R. This point of view was taken systematically in the book [7] where the particular importance of minimal polynomials (rather greater than that of characteristic polynomials) emerged quite clearly. That book also described several algorithms which use minimal polynomials as a crucial tool. The approach taken there was a good source of inspiration for our research, so we decided to delve into the theory of minimal polynomials, their uses, and their applications (for the details, see the full paper [6]).

First, we describe some algorithms for computing the minimal polynomial of an element of R and of a K-endomorphism of R. They refine similar algorithms examined in [7], and have been implemented and compared in CoCoALib [2].

We also address the problem of using a modular approach for computing minimal polynomials of elements of an affine $\mathbb{Q}$-algebra. As always with a modular approach, various obstacles have to be overcome (see for instance the discussion contained in [4] and in [5]). In particular, we deal with the notion of *reduction of an ideal modulo* p, and we introduce the *σ-denominator* of an ideal (for a term-ordering σ). Then we show that almost all primes are *good* which paves the way to the construction of the modular algorithm, and we reconstruct the rational polynomial using fault-tolerant rational reconstruction [1].

Minimal polynomials can be successfully and efficiently used to compute several important invariants of zero-dimensional affine K-algebras. More specifically, we describe some algorithms which show respectively how to determine whether a zero-dimensional ideal is radical, and how to compute the radical of a zero-dimensional ideal. Then we present some algorithms which determine whether a zero-dimensional ideal is maximal or primary. The techniques used depend very much on the field K. The main distinction is between small finite fields and fields of characteristic zero or

big fields of positive characteristic. In particular, it is noteworthy that in the first case Frobenius spaces play a fundamental role.

Finally, we describe how to compute the primary decomposition of a zero-dimensional affine K-algebra. They are inspired by the content of Chapter 5 of [7], but they present many novelties.

All these algorithms have been implemented in CoCoALib [2], and are accessible from CoCoA [3]. Their merits are also illustrated by good timings.

This research was partly supported by the project H2020-FETOPN-2015-CSA_712689 of the European Union

Keywords: Minimal polynomial, Gröbner bases, elimination, primary decomposition, radical.

References

[1] J. Abbott, *Fault-Tolerant Modular Reconstruction of Rational Numbers*, J. Symb. Comp. **80** (2017), pp. 707–718.

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

[3] J. Abbott, A.M. Bigatti, L. Robbiano, *CoCoA: a system for doing Computations in Commutative Algebra.* Available at `http://cocoa.dima.unige.it`

[4] J. Abbott, A.M. Bigatti, L. Robbiano, *Implicitization of Hypersurfaces*, J. Symb. Comput. **81** (2017), pp. 20–40.

[5] J. Abbott, A.M. Bigatti, L. Robbiano, *Ideals Modulo p*, `arxiv:1801.06112`, 2018

[6] J. Abbott, A. Bigatti, E. Palezzato, L. Robbiano, *Computing and Using Minimal Polynomials*, `arXiv:1704.03680`, 2017.

[7] M. Kreuzer and L. Robbiano, *Computational Linear and Commutative Algebra*, Springer, Heidelberg (2016).

[1]Dipartiment di Matematica
Università degli Studi di Genova
Via Dodecaneso 35, 16146, Genova
`abbott,bigatti@dima.unige.it`
`lorobbiano@gmail.com`

[2]Department of Mathematics
Hokkaido University
Kita 10, Nishi 8, Kita-Ku, Sapporo, Hokkaido, 060-0810
palezzato@math.sci.hokudai.ac.jp

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game.

Michela Ceria[1], **Teo Mora**[2]

In 1990 Cerlienco and Mureddu [4] gave a combinatorial algorithm which, given an ordered set of points $\underline{\mathbf{X}} = [P_1, ..., P_N] \subset \mathbf{k}^n$, $\mathbf{k}$ a field, returns the lexicographical Gröbner escalier $\underline{\mathsf{N}(I(\mathbf{X}))} \subset \mathcal{T} := \{x^\gamma := x_1^{\gamma_1} \cdots x_n^{\gamma_n} \,|\, \gamma := (\gamma_1, ..., \gamma_n) \in \mathbb{N}^n\}$ of the vanishing ideal $I(\mathbf{X}) := \{f \in \mathcal{P} : f(P_i) = 0, \forall i \in \{1, ..., N\}\} \subset \mathcal{P} := \mathbf{k}[x_1, ..., x_n]$. Such algorithm actually returns a bijection (labelled *Cerlienco-Mureddu correspondence* in [9, II,33.2]) $\Phi_{\underline{\mathbf{X}}} : \underline{\mathbf{X}} \to \underline{\mathsf{N}(I(\mathbf{X}))}$. The algorithm is inductive and thus has complexity $\mathcal{O}\left(n^2N^2\right)$, but it has the advantage of being iterative, in the sense that, given an ordered set of points $\underline{\mathbf{X}} = [P_1, ..., P_N]$, its related escalier $\underline{\mathsf{N}(I(\mathbf{X}))}$ and correspondence $\Phi_{\underline{\mathbf{X}}}$, for any point $Q \notin \underline{\mathbf{X}}$ it returns a term $\tau \in \mathcal{T}$ such that, denoting $\underline{\mathbf{Y}}$ the ordered set $\underline{\mathbf{Y}} := [P_1, ..., P_N, Q]$, $\underline{\mathsf{N}(I(\mathbf{Y}))} = \underline{\mathsf{N}(I(\mathbf{X}))} \sqcup \{\tau\}$, $\Phi_{\underline{\mathbf{Y}}}(P_i) = \Phi_{\underline{\mathbf{X}}}(P_i)$ for all i and $\tau = \Phi_{\underline{\mathbf{Y}}}(Q)$. In order to produce the lexicographical Gröbner escalier with a better complexity, [6] gave a completely different approach (*Lex Game*): given a set of (not necessarily ordered) points $\mathbf{X} = \{P_1, ..., P_N\} \subset \mathbf{k}^n$ they built a trie (*point trie*) representing the coordinates of the points and then used it to build a different trie, the *lex trie*, which allows to reed the lexicographical Gröbner escalier $\mathsf{N}(I(\mathbf{X}))$. Such algorithm has a very better complexity, $\mathcal{O}\left(nN + N\min(N, nr)\right)$, where $r < n$ is the maximal number of edges from a vertex in the point tree, but in order to obtain it, [6] was forced to give up iterativity. In 1982 Buchberger and Möller [2] gave an algorithm (*Buchberger-Möller algorithm*) which, for any term-ordering $<$ on $\mathcal{T}$ and any set of (not necessarily ordered) points $\mathbf{X} = \{P_1, ..., P_N\} \subset \mathbf{k}^n$ iterating on the $<$-ordered set $\mathsf{N}(I(\mathbf{X}))$, returns the Gröbner basis of $I(\mathbf{X})$ with respect to $<$, the set $\mathsf{N}(I(\mathbf{X}))$ and a family $[f_1, \cdots, f_N] \subset \mathcal{P}$ of separators of $\mathbf{X}$ *id est* a set of polynomials such that

$$f_i(P_j) = \delta_{ij} = \begin{cases} 0 & i \neq j \\ 1 & i = j. \end{cases}.$$

Later Möller [8] extended the same algorithm to any finite set of functionals defining a 0-dimensional ideal, thus absorbing also the FGLM-algorithm [5] and, on the other side, proving that Buchberger-Möller algorithm has the FGLM-complexity [5] $\mathcal{O}(n^2N^3f)$ where f is the average cost of evaluating a functional at a term*.

*A more precise evaluation was later given by Lundqvist, namely $\mathcal{O}(\min(n, N)N^3 + nN^2 + nNf + \min(n, N)N^2f)$.

Möller [8] gave also an alternative algorithm (*Möller algorithm*) which, for any term-ordering $<$ on $\mathcal{T}$, given an ordered set of points[†] $[P_1, ..., P_N] \subset \mathbf{k}^n$, for each $\sigma \leq N$, denoting $\mathbf{X}_\sigma = \{P_1, ..., P_\sigma\}$ returns, with complexity $\mathcal{O}(nN^3 + fnN^2)$

- the Gröbner basis of the ideal $I(\mathbf{X}_\sigma)$;
- the correlated escalier $\mathsf{N}(I(\mathbf{X}_\sigma))$;
- a term $t_\sigma \in \mathcal{T}$ such that $\mathsf{N}(I(\mathbf{X}_\sigma) = \mathsf{N}(I(\mathbf{X}_{\sigma-1})) \sqcup \{\tau\}$,
- a triangular set $\{q_1, \cdots, q_\sigma\} \subset \mathcal{P}$ s.t. $q_i(P_j) = \begin{cases} 0 & i < j \\ 1 & i = j, \end{cases}$
- whence a family of separators can be easily deduced by Gaussian reduction,
- a bijection Φ_σ such that $\Phi_\sigma(P_i) = \tau_i$ for each $i \leq \sigma$, which moreover if $<$ is lexicographical, then coincides with Cerlienco-Mureddu correspondence.

Later, Mora [9, II,29.4] remarked that, since the complexity analysis of both Buchberger-Möller and Möller algorithms were assuming to perform Gaussian reduction on an N-square matrix and to evaluate each monomial in the set $\mathsf{B}(I(\mathbf{X})) := \{\tau x_j, \tau \in \mathsf{N}(I(\mathbf{X}_\sigma)), 1 \leq j \leq n\}$ over each point $P_i \in \mathbf{X}$, within that complexity one can use all the informations which can be deduced by the computations $\tau(P_i), \tau \in \mathsf{B}(I(\mathbf{X})), 1 \leq i \leq N$; he therefore introduced the notion of *structural description* of a 0-dimensional ideal [9, II.29.4.1] and gave an algorithm which computes such structural description of each ideal $I(\mathbf{X}_\sigma)$. Also anticipating the recent mood of degroebnerizing effective ideal theory, Mora, in connection with Auzinger-Stetter matrices and algorithm [1], proposed to present a 0-dimensional ideal $I \subset \mathcal{P}$ and its quotient algebra $\mathcal{P}/I$ by giving its *Gröbner representation* [9, II.29.3.3] *id est* the assignment of a $\mathbf{k}$-linearly independent ordered set $[q_1, \ldots, q_N] \subset \mathcal{P}/I$ and n N-square matrices $\left(a_{lj}^{(h)}\right), 1 \leq h \leq n$, which satisfy

1. $\mathcal{P}/I \cong \mathrm{Span}_{\mathbf{k}}\{q_1, \ldots, q_N\}$,
2. $x_h q_l = \sum_j a_{lj}^{(h)} q_j, 1 \leq j, l \leq N, 1 \leq h \leq n.$

Since Möller algorithm and Mora's extension is inductive, our aim is to give an algorithm which given an ordered set of points $\mathbf{X} = [P_1, ..., P_N] \subset \mathbf{k}^n$ produces for each $\sigma \leq N$ the lexicographical Gröbner escalier $\mathsf{N}(I(\mathbf{X}_\sigma))$, the related Cerlienco-Mureddu correspondence, a family of squarefree separators for $\mathbf{X}_\sigma$, and the n N-square Auzinger-Stetter matrices $\left(a_{lj}^{(h)}\right), 1 \leq h \leq n$, which satisfy condition 2. above with respect the linear basis $\mathsf{N}(I(\mathbf{X}_\sigma))$. The advantage is that, any time

[†] Actually the algorithm is stated for an ordered finite set of functionals $[\ell_1, ..., \ell_N] \subset \mathrm{Hom}_{\mathbf{k}}(\mathcal{P}, \mathbf{k})$ such that for each $\sigma \leq N$ the set $\{f \in \mathcal{P} : \ell_i(f) = 0, \forall i \leq s\}$ is an ideal.

a *new* point is to be considered, the old data do not need to be modified and actually can simplify the computation of the data for the new ideal. Since the Lex Game approach which has no tool for considering the order of the points has no way of using the data computed for the ideal $I(\mathbf{X}_{\sigma-1})$ in order to deduce those for $I(\mathbf{X}_{\sigma})$, while Möller algorithm and Mora's extension are iterative on the ordered points and intrinsically produce Cerlienco-Mureddu correspondence, in order to achieve our aim, we need to obtain a variation of Cerlienco-Mureddu algorithm which is not inductive. Our tool is the Bar Code [3], essentially a reformulation of the point trie which describes in a compact way the combinatorial structure of a (non necessarily 0-dimensional) ideal; the Bar Code allows to remember and read those data which Cerlienco-Mureddu algorithm is forced to inductively recompute. Actually, once the point trie is computed as in [6] with inductive complexity $\mathcal{O}(N \cdot N\log(N)n)$, the application of the Bar Code allows to compute the lexicographical Gröbner escaliers $\mathsf{N}(I(\mathbf{X}_{\sigma}))$ and the related Cerlienco-Mureddu correspondences, with iterative complexity $\mathcal{O}(N \cdot (n + \min(N, nr))) \sim \mathcal{O}(N \cdot nr)$. The families of separators can be iteratively obtained using Lagrange interpolation via data easily deduced from the point trie as suggested in [6] with complexity $\mathcal{O}(N \cdot \min(N, nr))$. The computation of the Auzinger-Stetter matrices is based on Lundqvist result [7, Lemma 3.2] and can be inductively performed with complexity[‡] $\mathcal{O}\left(N \cdot (nN^2)\right)$.

Keywords: zero-dimensional ideal, Cerlienco-Mureddu algorithm, lex game

References

[1] W. AUZINGER; H.J. STETTER, An Elimination Algorithm for the Computation of all Zeros of a System of Multivariate Polynomial Equations. *I.S.N.M.* **86**, 11–30 (1988).

[2] H.M. MÖLLER; B. BUCHBERGER, The construction of multivariate polynomials with preassigned zeros, *L. N. Comp. Sci.* **144**, 24–31 (1982).

[3] M. CERIA, Bar Code for monomial ideals, submitted to Journal of Symbolic Computations, special issue for MEGA 2017.

[4] L. CERLIENCO L.; M. MUREDDU, From algebraic sets to monomial linear bases by means of combinatorial algorithms. *Discrete Math.* **139**, 73-87 (1995).

[5] J.C. FAUGÈRE; P. GIANNI; D. LAZARD D; T. MORA, Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. *J.S.C.* **16**, 329–344 (1993).

[‡]Naturally, our decision of giving an algorithm which can produce data for the vanishing ideal when a new point is considered forbid us of using the new better algorithms for matrix multiplication; thus our complexity is $\mathcal{O}\left(N^3\right)$ and not $\mathcal{O}\left(N^{\omega}\right), \omega < 2.39$.

[6] B. FELSZEGHY; B. RÁTH; L. RÓNYAI The lex game and some applications. *J.S.C.* **4**, 663-681 (2006).

[7] S. LUNDQVIST, Vector space bases associated to vanishing ideals of points. *J.P.A.A.* **214**(4), 309-321 (2010).

[8] M.G. MARINARI; T. MORA; H.M. MÖLLER, Gröbner bases of ideals defined by functionals with an application to ideals of projective points. *J. AAECC* **4**, 103-145 (1993).

[9] T. MORA Solving Polynomial Equation Systems (4 Vols.). Cambridge Univ. Press, Cambridge, 2003–16.

[1]Department of Computer Science
University of Milan
Via Comelico 39, Milano, Italy
michela.ceria@gmail.com

[2]Department of Mathematics
University of Genoa
Via Dodecaneso 35
theomora@disi.unige.it

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Subschemes of the Border Basis Scheme

Martin Kreuzer[1], **Le Ngoc Long**[1], **Lorenzo Robbiano**[2]

All 0-dimensional ideals in a polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K having a fixed colength μ are parametrized by the Hilbert scheme $\mathrm{Hilb}^\mu(\mathbb{A}^n)$. Since it is not easy to find the equations defining these moduli schemes, we may opt to study border basis schemes. They are open subschemes of the Hilbert scheme which cover it and can be defined using easily computable quadratic equations.

More precisely, let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an *order ideal*, i.e. a divisor closed finite subset of the set of terms in P, and let $\partial\mathcal{O} = \{b_1, \ldots, b_\nu\}$ be the *border* of $\mathcal{O}$ which is defined by $\partial\mathcal{O} = (x_1\mathcal{O} \cup \cdots \cup x_n\mathcal{O}) \setminus \mathcal{O}$. After introducing new indeterminates c_{ij} for $1 \leq i \leq \mu$ and $1 \leq j \leq \nu$, we form the *generic $\mathcal{O}$-border prebasis* $G = \{g_1, \ldots, g_\nu\}$, where $g_j = b_j - \sum_{i=1}^{\mu} c_{ij}\, t_i$, and the *generic formal multiplication matrices* $\mathcal{A}_r = (a_{ij}^{(r)}) \in \mathrm{Mat}_\mu(K[c_{ij}])$, where

$$a_{ij}^{(r)} \;=\; \begin{cases} \delta_{im} & \text{if } x_r t_j = t_m \\ c_{im} & \text{if } x_r t_j = b_m \end{cases}$$

for $r = 1, \ldots, n$. It is well-known that the substitution of concrete values $c_{ij} \mapsto \gamma_{ij}$ with $\gamma_{ij} \in K$ into G yields an *$\mathcal{O}$-border basis* G_Γ, i.e. a system of generators of $I_\Gamma = \langle G_\Gamma \rangle$ such that the terms in $\mathcal{O}$ represent a vector space basis of P/I_Γ if and only if the commutators of $\mathcal{A}_1, \ldots, \mathcal{A}_n$ vanish at the point $\Gamma = (\gamma_{ij}) \in K^{\mu\nu}$. Hence the ideal $I(\mathbb{B}_\mathcal{O})$ generated by the entries of these commutators defined a subscheme $\mathbb{B}_\mathcal{O}$ of $\mathbb{A}^{\mu\nu}$ whose K-rational points correspond 1–1 to the 0-dimensional ideals of colength μ having an $\mathcal{O}$-border basis. This scheme is called the *$\mathcal{O}$-border basis scheme*, and given $\mathcal{O}$, its vanishing ideal is easy to compute. It has been studied previously in [1] and [2].

Having a good parametrization of all 0-dimensional ideals of a given colength invites the question how one can describe the loci of ideals with certain additional properties, e.g. algebraic properties such as defining a Gorenstein ring, or geometric properties such as the Cayley-Bacharach property. Based on the algorithms developed in [3] and on further characterizations, e.g. of the properties of being strictly Gorenstein or a strict complete intersection, we develop algorithms for computing the defining ideals of a number of subschemes of the border basis scheme $\mathbb{B}_\mathcal{O}$.

The first and most straightforward one is the locus of all 0-dimensional ideals I_Γ such that P/I_Γ is a (locally) Gorenstein ring. It was given in [3], Alg. 5.4 and uses the facts that this property is characterized by having a cyclic canonical module and that the multiplication maps on the canonical module are given by the transposes of the multiplication maps on the ring.

A more tricky case is the property of P/I_Γ to be a *strict Gorenstein ring*, i.e. of its graded ring $\mathrm{gr}_{\mathcal{F}}(P/I_\Gamma)$ with respect to the degree filtration $\mathcal{F}$ to be a Gorenstein local ring. In this case we can use the characterization which says that P/I_Γ has to have a symmetric affine Hilbert function and the Cayley-Bacharach property. However, both of these conditions require us to fix the Hilbert function.

The closed subscheme of $\mathbb{B}_\mathcal{O}$ whose K-rational points Γ correspond to rings P/I_Γ whose affine Hilbert function is dominated by a given Hilbert function $\mathcal{H}$ is called the *$\overline{\mathcal{H}}$-subscheme* of $\mathbb{B}_\mathcal{O}$ and is denoted by $\mathbb{B}_\mathcal{O}(\overline{\mathcal{H}})$. The open subscheme of $\mathbb{B}_\mathcal{O}(\overline{\mathcal{H}})$ whose K-rational points Γ correspond to rings P/I_Γ having exactly the affine Hilbert function $\mathcal{H}$ is denoted by $\mathbb{B}_\mathcal{O}(\mathcal{H})$. Both for $\mathbb{B}_\mathcal{O}(\overline{\mathcal{H}})$ and for the complement of $\mathbb{B}_\mathcal{O}(\mathcal{H})$ inside $\mathbb{B}_\mathcal{O}(\overline{\mathcal{H}})$ we provide explicit algorithms to calculate their defining equations. Thus we may operate on the set of ideals having a fixed Hilbert function.

The most useful of these sets is the *degree filtered $\mathcal{O}$-border basis scheme* $\mathbb{B}_\mathcal{O}^{\mathrm{df}}$ which corresponds to the Hilbert function of $\mathcal{O}$ itself. In this setting we provide explicit algorithms for calculating the locus of all points Γ such that P/I_Γ has the Cayley-Bacharach property, and then the locus corresponding to the strict Gorenstein rings P/I_Γ mentioned above.

Finally, we consider the locus corresponding to all strict complete intersection ideals I_Γ, i.e. to all such ideals for which the degree form ideal $\mathrm{DF}(I_\Gamma)$ is generated by a homogeneous regular sequence. To characterize this locus, we use a suitable version of an old result by Wiebe (see [4], Satz 3) which says that a local ring R with maximal ideal $\mathfrak{m}$ is a complete intersection if and only if the 0-th Fitting ideal of $\mathfrak{m}$ satisfies $\mathrm{Fitt}_0(\mathfrak{m}) \neq \langle 0 \rangle$. Based on a parametrization of all rings $P/\mathrm{DF}(I_\Gamma)$ using the *homogeneous $\mathcal{O}$-border basis scheme*, we succeed in constructing a version of Wiebe's result which works for families of 0-dimensional ideals and allows us to describe the locus of all strict complete intersections in the moduli space via explicit polynomial equations.

Keywords: border basis, Gorenstein ring, complete intersection

References

[1] M. KREUZER AND L. ROBBIANO, Deformations of border bases. *Coll. Math.* **59**, 275–297 (2008).

[2] M. KREUZER AND L. ROBBIANO, The geometry of border bases. *J. Pure Appl. Alg.* **215**, 2005–2018 (2011).

[3] M. KREUZER, L.N. LONG AND L. ROBBIANO, On the Cayley-Bacharach property. *arxiv:1804.09469* [math.AC] (2018).

[4] H. WIEBE, Über homologische Invarianten lokaler Ringe (in German). *Math. Ann.* **179**, 257–274 (1969).

[1]Faculty of Informatics and Mathematics
University of Passau
D-94030 Passau, Germany
martin.kreuzer@uni-passau.de,
nglong16633@gmail.com

[2]Dipartimento di Matematica
Università di Genova
Via Dodecaneso 35
I-16146 Genova, Italy
lorobbiano@gmail.com

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Fast Gröbner basis computation and polynomial reduction in the generic bivariate case

Joris van der Hoeven[1], **Robin Larrieu**[1]

Let $A, B \in \mathbb{K}[X, Y]$ be two bivariate polynomials over an effective field $\mathbb{K}$, and let G be the reduced Gröbner basis of the ideal $I := \langle A, B \rangle$ generated by A and B with respect to the usual degree lexicographic order. Assuming A and B sufficiently generic, we design a quasi-optimal algorithm for the reduction of $P \in \mathbb{K}[X, Y]$ modulo G, where "quasi-optimal" is meant in terms of the size of the input A, B, P. Immediate applications are an ideal membership test and a multiplication algorithm for the quotient algebra $\mathbb{A} := \mathbb{K}[X, Y]/\langle A, B \rangle$, both in quasi-linear time. Moreover, we show that G itself can be computed in quasi-linear time with respect to the output size.

Keywords: Polynomial reduction, Gröbner basis, Complexity, Algorithm

References

[1] JORIS VAN DER HOEVEN; ROBIN LARRIEU, Fast Gröbner basis computation and polynomial reduction in the generic bivariate case. Preprint at `https://hal.archives-ouvertes.fr/hal-01770408/`

[2] JORIS VAN DER HOEVEN; ROBIN LARRIEU, Fast reduction of bivariate polynomials with respect to sufficiently regular Gröbner bases. Proceedings *ISSAC 2018* (to appear). Preprint at `http://hal.archives-ouvertes.fr/hal-01702547`.

[1]Laboratoire d'informatique de l'École polytechnique
LIX, UMR 7161 CNRS
Campus de l'École polytechnique
1, rue Honoré d'Estienne d'Orves
Bâtiment Alan Turing, CS35003
91120 Palaiseau, France
`vdhoeven@lix.polytechnique.fr`
`larrieu@lix.polytechnique.fr`

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

De Nugis Groebnerialium 5: Noether, Macaulay, Jordan*

Teo Mora[1]

The true power of Lasker-Noether decomposition theorem grants that each ideal in a Noetherian ring has an irredundant (and reduced) representation as finite intersection of *irreducible* primary ideals and, in the polynomial ring over a field, there is an algorithm (due to Macaulay) which effectively computes such decomposition. Moreover, once a frame of coordinates is fixed, such decomposition is unique. I am wondering since years whether this result could allow to define (if and when it exists) an *intrinsic coordinate frame* for primary ideals. Recently I realized that generalized eigenvectors could be a potential solution, thus allowing me to give a potential definition.

In connection with Lasker-Noether primary decomposition, Emmy Noether stated [4] that

Definition 1 (Noether)**.** Let R be a commutative ring with unity and let $\mathfrak{a} \subset R$ be an ideal.

$\mathfrak{a}$ is said to be

- *reducible* if there are two ideals $\mathfrak{b}, \mathfrak{c} \subset R$ such that $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}, \mathfrak{b} \supset \mathfrak{a}, \mathfrak{c} \supset \mathfrak{a}$;
- *irreducible* if it is not reducible.

Proposition 2 (Lasker–Noether)**.** *In a Noetherian ring R each ideal $\mathfrak{f} \subset R$ is a finite intersection of irreducible ideals: $\mathfrak{f} = \cap_{i=1}^{r} \mathfrak{i}_i$.*

Definition 3 (Noether)**.** Let R be a Noetherian ring and $\mathfrak{f} \subset R$ an ideal. A representation $\mathfrak{f} = \cap_{i=1}^{r} \mathfrak{i}_i$, of $\mathfrak{f}$ as intersection of finite irreducible ideals is called a *reduced representation* if, for each $I, 1 \leq I \leq r$,

- $\mathfrak{i}_I \not\supseteq \bigcap\limits_{\substack{i=1 \\ i \neq I}}^{r} \mathfrak{i}_i$, and
- there is no irreducible ideal $\mathfrak{i}'_I \supset \mathfrak{i}_I$ such that $\mathfrak{f} = \left(\bigcap\limits_{\substack{i=1 \\ i \neq I}}^{r} \mathfrak{i}_i \right) \bigcap \mathfrak{i}'_I$. □

*This note was devised while attending to the CIRM, Luminy, *Workshop Symmetry and Computational*; thanks to the organizers for the hospitality and stimulation. I am also grateful to Elisa Gorla which pointed me to Jordan blocks and Michela Ceria for fruitable discussions.

Proposition 4 (Noether)**.** *In a Noetherian ring R, each ideal $\mathfrak{f} \subset R$ has a reduced representation as intersection of finite irreducible ideals.*

Let us denote $\mathcal{P} := K[X_1, \cdots, X_n]$ the polynomial ring over the field K and

$$\mathcal{T} := \{X_1^{a_1}, \cdots, X_n^{a_n} : (a_1, \cdots, a_n) \in \mathbb{N}\}.$$

Example 5 (Hentzelt). 1. The decompositions

$$(X^2, XY) = (X) \cap (X^2, XY, Y^\lambda), \text{ for each } \lambda \in \mathbb{N}, \lambda \geq 1,$$

where $\sqrt{(X^2, XY, Y^\lambda)} = (X, Y) \supset (X)$, show that embedded components are not unique; however, $(X^2, Y) \supseteq (X^2, XY, Y^\lambda)$, for each $\lambda > 1$, shows that (X^2, Y) is a reduced embedded irreducible component and that $(X^2, XY) = (X) \cap (X^2, Y)$ is a reduced representation.

2. The decompositions $(X^2, XY) = (X) \cap (X^2, Y + aX)$, for each $a \in \mathbb{Q}$, where $\sqrt{(X^2, Y + aX)} = (X, Y) \supset (X)$, and, clearly, each $(X^2, Y + aX)$ is reduced, show that also reduced representation is not unique; remark that, setting $a = 0$ we find again the decomposition $(X^2, XY) = (X) \cap (X^2, Y)$ found above.

This set of examples suggested Emmy Noether to intersect all irreducible components which share the same associated prime and to distinguish primaries between *embedded* and *isolated* in order to give her uniqueness result on irredundant primary representation.

Some time before, Macaulay [3], through his theory of *inverse systems* and *dialytic arrays* studied the inner structure of $(X_1, \ldots, X_n)$-primary ideals at the origin in the polynomial ring $K[X_1, \cdots, X_n] =: \mathcal{P}$ giving an efficient algorithm which later Gröbner [2, pp.177–178] realized was computing the reduced representation of a $(X_1, \ldots, X_n)$-primary ideal and which can be easily generalized to [5, II.Corollary 32.3.3] produce a reduced representation of each $(X_1, \ldots, X_n)$-closed ideal.

Example 6. Given the monomial ideal $I := (X^3, XY, Y^3)$ Macaulay starts with the functionals $M(t)(\cdot), t \in \mathcal{T}$ which associate to each polynomial the coefficient of t in its expansion, the *escalier* $\mathcal{T}/I$ and the "corners" X^3, Y^3 getting the two modules

$$\mathrm{Span}_K\{M(X^2), XM(X^2), X^2M(X^2)\} = \mathrm{Span}_K\{M(X^2), M(X), M(1)\}$$

and $\mathrm{Span}_K\{M(Y^2), YM(Y^2), Y^2M(Y^2)\} = \mathrm{Span}_K\{M(Y^2), M(Y), M(1)\}$ which are dual to the ideals (X^3, Y) and (X, Y^3) whence $I = (X^3, Y) \cap (X, Y^3)$.

Notwithstanding Hentzelt's example, Macaulay's solution in a sense is "unique"; namely it depends on a precise frame of coordinates, since each component is computed by Macaulay essentially by repeatedly multiplying some functionals by the variables.

Example 7. The ideal $(X_1, X_2)^2$ has all the irreducible decompositions

$$(X_1, X_2)^2 = ((aX + bY)^2, cX + dY) \cap (aX + bY, (cX + dY)^2), ad - cb = 1.$$

Example 8. Apparently, Example 7 is all one needs to dismiss the question posed on the title; however if we consider any linear form $\ell \in K[X_1, X_2, X_3]$ s.t. $\mathrm{Span}_K = \{X_1, X_2, \ell\} = \mathrm{Span}_K = \{X_1, X_2, X_3\}$ we realize that in the (X_1, X_2, X_3)-primary ideal

$$\begin{aligned} J &:= (X_1, X_2, X_3)^2 \cap (X_1, X_2, \ell^3) \\ &= (X_1^2, X_1X_2, X_2^2, X_1X_3, X_2X_3, X_3^3) \\ &= ((aX + bY)^2, cX + dY, X_3) \cap (aX + bY, (cX + dY)^2, X_3) \cap (X_1, X_2, \ell^3) \end{aligned}$$

the coordinate X_3 plays a rôle at least as the direction of the plane (X_1, X_2).

Let us consider a $(X_1, \ldots, X_n)$-primary ideal $I \subset K[X_1, \cdots, X_n] =: \mathcal{P}$, the unique order ideal $\mathbf{N}(I) \subset \mathcal{T}$ such that $\mathrm{Span}_K\{\mathbf{N}(I)\} = \mathcal{P}/I$, a linear form

$$\ell \in \mathrm{Span}_K\{X_1, \cdots, X_n\} =: \mathcal{B}_1,$$

the Auzinger-Stetter[1] matrix A describing the effect of the morphism $A \to A : f \mapsto \ell f$ on $\mathbf{N}(I)$ and its Jordan normal form J.

Denoting, for $k, 1 \leq k \leq \#\mathbf{N}(J)$, $\rho_k := \mathrm{rank}(A^{k-1}) - \mathrm{rank}(A^k)$, $\mu_0 := \rho_1$ and $\mu_i := \rho_i - \rho_{i+1}$ for each $i, 1 \leq i < l := max(k : \rho_k \neq 0)$. Note that $\mu_0 = \sum_{i>0} \mu_i = \#\mathcal{B}_1 = n$ is the number of Jordan blocks of J. Note also that the following conditions are equivalent

1. there are n values $i_1 > i_2 > \ldots > i_n$ with $\mu_{i_j} = 1$,
2. $\mu_i \in \{0, 1\}$ for each i.

If this happens we can choose n generalized eigenvectors v_j each of ranks i_j in a such way that the eigenvectors $w_j := A^{i_j - 1}v_j$ satisfy $\mathrm{Span}_K\{w_1, \cdots, w_n\} =: \mathcal{B}_1$ and we can inductively choose each w_j in such a way that the basis $\{w_1, \cdots, w_n\}$ is orthogonal.

Definition 9. If the conditions above are satisfied the ordered set $\{w_1, \cdots, w_n\}$ is called the *intrinsic coordinate frame* for the $(X_1, \ldots, X_n)$-primary ideal I.

Of course this definition requires to settle technical problems which Numerical Analysis can answer, starting from the crucial questions: is this frame "unique" and in which sense? ℓ must be "generic" in some sense, but in which sense? Example 8 suggests that we can assume to have ℓ in a Zariski open.

The other problem is to consider a $(X_1, \ldots, X_n)$-closed ideal I with the origin as singular point and study if the application of this tecnique to sufficiently many ideals $I \cap (X_1, \ldots, X_n)^d$ can impose an intrinsic coordinate frame at the singular point of I, following the track of computation for the ideal $I = (X_1^3 - X_1^2 - X_2^2)$ performed in [5, II.Examples 32.4.2,32.7.1].

Keywords: 0-dimensional primaries, primary decomposition, Jordan blocks

References

[1] W. AUZINGER; H.J. STETTER, An Elimination Algorithm for the Computation of all Zeros of a System of Multivariate Polynomial Equations. *I.S.N.M.* **86**, 11–30 (1988)

[2] W. GRÖBNER W., *Moderne Algebraische Geometrie II*. Bibliographische Institut, Mannheim, 1970.

[3] F. S. MACAULAY, *The Algebraic Theory of Modular Systems*, Cambridge Univ. Press, Cambridge, 1916.

[4] E. NOETHER, Idealtheorie in Ringbereichen. *Math. Annales* **83**, 25–66 (1921).

[5] T. MORA Solving Polynomial Equation Systems (4 Vols.). Cambridge Univ. Press, Cambridge, 2003–16.

[1]Department of Mathematics
University of Genoa
Via Dodecaneso 35
theomora@disi.unige.it

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Solving and bonding 0-dimensional ideals: Möller Algorithm and Macaulay Bases

Teo Mora[1]

Denote by $\mathcal{P} := \mathbf{k}[x_1, ..., x_n]$ the polynomial ring over the field $\mathbf{k}$, by $\bar{\mathbf{k}}$ the algebraic closure of $\mathbf{k}$, by $\mathbf{m} = (x_1, ..., x_n) \subset \mathcal{P}$ the maximal ideal at the origin and by

$$\mathcal{T} := \{x^\gamma := x_1^{\gamma_1} \cdots x_n^{\gamma_n} \,|\, \gamma := (\gamma_1, ..., \gamma_n) \in \mathbb{N}^n\}$$

the semigroup of terms in $\mathcal{P}$ which is its "natural" basis as a $\mathbf{k}$-vector space.

The $\mathbf{k}$-vector space of the linear morphisms $L : \mathcal{P} \to \mathbf{k}$, $\hat{\mathcal{P}} = \mathrm{Hom}_{\mathbf{k}}(\mathcal{P}, \mathbf{k})$ has a natural structure as $\mathcal{P}$-module which is obtained by defining, for each $\ell \in \hat{\mathcal{P}}$ and $f \in \mathcal{P}$, $\ell \cdot f \in \hat{\mathcal{P}}$ as

$$g \mapsto (\ell \cdot f)(g) = \ell(fg), \forall g \in \mathcal{P}.$$

Macaulay [4, 5] under the notion of *inverse system* proposed a representation of $\hat{\mathcal{P}}$ as a series ring $\mathbf{k}[[x_1^{-1}, ..., x_n^{-1}]]$ and specialized his approach in order to describe, under the name of *Noetherian equations*, the structure of both $\mathbf{m}$-primary ideals at the origin and $\mathbf{m}$-closed* ideals. In order to do so he restricted himself to the polynomial ring

$$\mathcal{P} = \mathbf{k}[x_1, ..., x_n] \cong \mathbf{k}[x_1^{-1}, ..., x_n^{-1}] \subset \mathbf{k}[[x_1^{-1}, ..., x_n^{-1}]] = \hat{\mathcal{P}} = \mathrm{Hom}_{\mathbf{k}}(\mathcal{P}, \mathbf{k})$$

representing it as the $\mathbf{k}$-vector space $\mathrm{Span}_{\mathbf{k}}(\mathbb{M})$ generated by the set $\mathbb{M} = \{M(\tau) : \tau \in \mathcal{T}\}$ of functionals bihortogonal to the set $\mathcal{T}$ defined by

$$M(\tau) : \mathcal{P} \to \mathbf{k}, \quad f = \sum_{t \in \mathcal{T}} c(f,t)t \mapsto c(f,t), \forall f \in \mathcal{P},$$

so that each polynomial $f \in \mathcal{P}$ is represented as $f = \sum_{\tau \in \mathcal{T}} M(\tau)\tau$. In order to impose a $\mathcal{P}$-module structure on it, he defined, for each $j, 1 \le j \le n$, the linear maps

$$\sigma_j : \mathrm{Span}_{\mathbf{k}}(\mathbb{M}) \to \mathrm{Span}_{\mathbf{k}}(\mathbb{M}), \quad \tau \mapsto \sigma_j(M(\tau)) := \begin{cases} M(\omega) & \text{if } \tau = x_j\omega \\ 0 & \text{if } x_j \nmid \tau; \end{cases}$$

since it holds $\sigma_i\sigma_j = \sigma_j\sigma_i$ for each pair $1 \le i, j \le n$, this, for each $\upsilon = x_1^{\gamma_1} \cdots x_n^{\gamma_n} \in \mathcal{T}$, defines a unique map

$$\sigma_\upsilon := \sigma_1^{\gamma_1} \cdots \sigma_n^{\gamma_n} : \mathrm{Span}_{\mathbf{k}}(\mathbb{M}) \to \mathrm{Span}_{\mathbf{k}}(\mathbb{M}), \quad \tau \mapsto \sigma_\upsilon(M(\tau)) := \begin{cases} M(\omega) & \text{if } \tau = \upsilon\omega \\ 0 & \text{if } \upsilon \nmid \tau. \end{cases}$$

*id est ideals $I \subset \mathcal{P}$ s.t. $I = \bigcup_d I + \mathbf{m}^d$.

Therefore for each $f = \sum_{t\in\mathcal{T}} c(f,t)t \in \mathcal{P}$ a map $\sigma_f : \mathrm{Span}_{\mathbf{k}}(\mathbb{M}) \to \mathrm{Span}_{\mathbf{k}}(\mathbb{M})$ is uniquely defined as $\sigma_f = \sum_{t\in\mathcal{T}} c(f,t)\sigma_t$ and under this definition $\mathrm{Span}_{\mathbf{k}}(\mathbb{M})$ is naturally endowed with the $\mathcal{P}$-module structure defined by

$$\ell \cdot f := \sigma_f(\ell) \in \mathrm{Span}_{\mathbf{k}}(\mathbb{M}), \forall \ell \in \mathrm{Span}_{\mathbf{k}}(\mathbb{M}), f \in \mathcal{P}.$$

Definition 10. A vector subspace $\Lambda \subset \mathrm{Span}_{\mathbf{k}}(\mathbb{M})$ is called

- x_j*-stable* if for each $\ell \in \Lambda, \sigma_j(\ell) \in \Lambda$;
- *stable* if for each $\ell \in \Lambda$ and each $f \in \mathcal{P}, \sigma_f(\ell) \in \Lambda$. □

Lemma 11. *Any vector subspace $\Lambda \subset \mathrm{Span}_{\mathbf{k}}(\mathbb{M})$ is stable iff it is x_j-stable, for each j.*

Theorem 12. *Let $\Lambda \subset \mathrm{Span}_{\mathbf{k}}(\mathbb{M}) \subset \hat{\mathcal{P}}$ be any finite dimensional* $\mathbf{k}$*-vector subspace. Then, the following conditions are equivalent:*

1. *Λ is stable.*
2. *the vector space $\mathfrak{I}(\Lambda) := \{f \in \mathcal{P} : \ell(f) = 0, \forall \ell \in \Lambda\} \subset \mathcal{P}$ is an ideal and $\mathfrak{I}(\Lambda) \subset \mathbf{m}$.*

Denoting, for each $\mathbf{k}$-vector subspace $P \subset \mathcal{P}$,

$$\mathfrak{M}(P) := \{\ell \in \mathrm{Span}_{\mathbf{k}}(\mathbb{M}) : \ell(f) = 0, \forall f \in P\} \subset \mathrm{Span}_{\mathbf{k}}(\mathbb{M})$$

it holds

Theorem 13. *The mutually inverse maps $\mathfrak{I}(\cdot)$ and $\mathfrak{M}(\cdot)$ give a biunivocal, inclusion reversing, correspondence between the set of the* $\mathbf{m}$*-closed ideals $I \subset \mathcal{P}$ and the set of the stable* $\mathbf{k}$*-sub vector spaces $\Lambda \subset \mathrm{Span}_{\mathbf{k}}(\mathbb{M})$.* □

Gröbner[3] gave a natural description of each functional $M(\tau) \in \mathbb{M}$ in terms of differential operations, setting, for each $(i_1, \ldots, i_n) \in \mathbb{N}^n$, $\tau := x_1^{i_1} \ldots x_n^{i_n}$ and denoting

$$D(\tau) := D(i_1, \ldots, i_n) : \mathcal{P} \to \mathcal{P}$$

the differential operator $D(\tau) := D(i_1, \ldots, i_n) = \frac{1}{i_1! \cdots i_n!} \frac{\partial^{i_1+\cdots+i_n}}{\partial x_1^{i_1} \cdots \partial x_n^{i_n}}$, so that, for each $\tau \in \mathcal{P}$, it holds $M(\tau)(\cdot) = D(\tau)(\cdot)(0, \ldots, 0)$.

Gröbner's formulation has the only weakness of requiring that $(\mathbf{k}) = 0$, but this problem is trivially fixed using the Hesse derivates $D_i^{(j)}(x_i^m) = \begin{cases} \binom{m}{j} x^{m-j} & \text{if } m \geq j \\ 0 & \text{if } m < j \end{cases}$ thus obtaining $M(\tau)(\cdot) = D_1^{(i_1)} \cdots D_n^{(i_n)}(\cdot)(0, \ldots, 0)$.

Given a termordering $<$ on $\mathcal{T}$, for each $\ell = \sum_{v\in\mathcal{T}} \xi(v,\ell)v$ we denote

$$\mathbf{T}_<(\ell) := \min_< (v : \xi(v,\ell) \neq 0) .$$

Definition 14. [1] Let $I \subset \mathcal{P}$ be an $\mathbf{m}$-closed ideal. A $\mathbf{k}$-basis $\{\ell_1, \ell_2, \ldots, \ell_i, \ldots\}$ of the stable $\mathbf{k}$-sub vector space $\Lambda := \mathfrak{M}(I)$ is called the *Macaulay basis* of Λ w.r.t. a termordering $<$ if

- $\mathbf{T}_<\{\Lambda\} := \{\mathbf{T}_<(\ell_i)\} \subset \mathcal{T}\}$ is an order ideal;
- $\ell_i = M(\mathbf{T}_<(\ell_i)) + \sum_{v \in \mathcal{T} \setminus \mathbf{T}_<(\Lambda)} \xi(v, \ell_i) v$ for suitable $\xi(v, \ell_i) \in \mathbf{k}$ and for each i. □

Given a 0-dimensional ideal $I \subset \mathcal{P}$ there are different techniques for computing its roots $\mathfrak{Z}(I) \subset \bar{\mathbf{k}}^n$ (see [9, III]) and, for each such root $\mathsf{a} \in \mathfrak{Z}(I)$, the correlated primary component of I (see [9, II.ch.35]); given an $\mathbf{m}$-closed ideal through any finite (not necessarily Gröbner) basis, [7] (see also [1]) computes, for any $\delta \in \mathbb{N}$, the Macaulay basis of $\bigcup_{d \leq \delta} I + \mathbf{m}^d$.

The procedure given by Macaulay [5] allows to produce the irreducible reduced decomposition of any $\mathbf{m}$-primary ideal.

The converse problem can be stated as

> given a finite set $\mathcal{Z} \subset \mathbf{k}^n$ and, for each $\mathsf{a} = (a_1, \ldots, a_n) \in \mathcal{Z}$, denoting
>
> $$\lambda_{\mathsf{a}} : \mathcal{P} \to \mathcal{P} \quad f(x_1, \ldots, x_n) \mapsto f(x_1 + a_1, \ldots, x_n + a_n),$$
>
> a stable $\mathbf{k}$-sub vector spaces $\Lambda_{\mathsf{a}} \subset \mathrm{Span}_{\mathbf{k}}(\mathbb{M})$ describe the 0-dimensional ideal $I = \bigcap_{\mathsf{a} \in \mathcal{Z}} \lambda_{\mathsf{a}}^{-1} (\mathfrak{I}(\Lambda_{\mathsf{a}}))$

Möller Algorithm [6] solves it; actually given any finite set of linearly independent functionals $\{\ell_1, \ldots, \ell_N\}$ properly ordered so that each sub vector space $L_i = \{\ell_1, \ldots, \ell_i\}, 1 \leq i \leq N$ is a $\mathcal{P}$-module so that each $I_i := \mathfrak{I}(L_i)$ is a 0-dimensional ideal, for each i returns the separators of the functionals L_i, the *Gröbner represantion* [9, II.29.3.3;III.pg.xvi] of each ideal I_i, producing in particular the order ideal (*escalier*) $\mathbf{N}(I_i)$ which is a $\mathbf{k}$-basis of the algebra $\mathcal{P}/I_i$ and also [8] the related Cerlienco–Mureddu Correspondence[†]

References

[1] M.E. ALONSO; M.G. MARINARI; T. MORA, The Big Mother of All the Dualities, II: Macaulay Bases. *J. AAECC* **17**, 409–451 (2006).

[2] M. CERIA; T. MORA Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game. This issue.

[3] W. GRÖBNER W., *Algebraische Geometrie II*. Bibliographische Institut, Mannheim, 1970.

[†] So in particular the results discussed in [2] hold for any 0-dimensional ideal.

[4] F. S. MACAULAY, On the Resolution of a given Modular System into Primary Systems including some Properties of Hilbert Numbers. *Math. Ann.* **74**,66–121 (1913).

[5] F. S. MACAULAY, *The Algebraic Theory of Modular Systems*, Cambridge Univ. Press, Cambridge, 1916.

[6] M.G. MARINARI; T. MORA; H.M. MÖLLER, Gröbner bases of ideals defined by functionals with an application to ideals of projective points. *J. AAECC* **4**, 103-145 (1993).

[7] M.G. MARINARI; T. MORA; H.M. MÖLLER, On multiplicities in Polynomial System Solving. *Trans. AMS* **348**, 3283–3321 (1996).

[8] M.G. MARINARI; M.T. MORA, Cerlienco-Mureddu Correspondence and Lazard Structural Theorem. *Investication Operacional* **27**, 155-178 (2006).

[9] T. MORA Solving Polynomial Equation Systems (4 Vols.). Cambridge Univ. Press, Cambridge, 2003–16.

[1]Department of Mathematics
University of Genoa
Via Dodecaneso 35
theomora@disi.unige.it

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

On the computation of algebraic relations of bivariate polynomials

Simone Naldi[1], **Vincent Neiger**[1], and **Grace Younes**[2]

Computing algebraic relations (or syzygies) between multivariate polynomials is a central topic in computational commutative algebra. Given $f_1, \ldots, f_m \in K[X]$, $X = (X_1, \ldots, X_n)$, and a zero-dimensional ideal $I \subset K[X]$, this problem amounts to finding $p_1, \ldots, p_m \in K[X]$ satisfying

$$p_1 f_1 + \cdots + p_m f_m \in I.$$

More precisely, one goal is to compute a Gröbner basis of the module of all such relations. In some applications, for instance in decoding algorithms from coding theory, one just needs to compute one relation satisfying degree bounds which are given a priori.

A well known particular case is the computation of Padé approximants of polynomial functions $h \in K[X]$, namely $a, b \in K[X]$ satisfying $a = bh$ in the coordinate ring $K[X]/I$. This problem can be interpreted as a structured linear system of equations.

In the univariate case, iterative algorithms have been developed in [1, 6]. Similar algorithms appeared for the multivariate case for example in [2, 4], leading to complexity bounds that are cubic in the degree of I and linear in the number of variables.

For the computation of univariate relations, divide-and-conquer variants of the mentioned algorithms have been given in [1, 3, 5]. However, to the best of our knowledge no similar improvements have been obtained in multivariate settings. In this talk we will report on ongoing work aiming at algorithmic improvements in the bivariate case and for ideals I that have some special structure.

Keywords: Padé approximants, syzygies, structured matrices, divide and conquer

References

[1] BECKERMANN, B., LABAHN, G. A uniform approach for the fast computation of matrix-type Padé approximants. *SIAM Journal on Matrix Analysis and Applications*, 15(3), 804-823 (1994).

[2] P. FITZPATRICK, Solving a multivariable congruence by change of term order. *J. Symb. Comp.* **24** 575–589 (1997).

[3] GIORGI, P., JEANNEROD, C. P., VILLARD, G. On the complexity of polynomial matrix computations. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation* pp. 135-142 (2003, August).

[4] MARINARI, M. G., MOELLER, H. M., MORA, T. 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).

[5] V. NEIGER, V.T. XUAN, Computing canonical bases of modules of univariate relations. *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, Kaiserslautern, Germany, July 2017.

[6] VAN BAREL, M., BULTHEEL, A. A general module theoretic framework for vector M-Padé and matrix rational interpolation. *Numerical Algorithms*, 3(1), 451-461 (1992).

[1]XLIM
Université de Limoges
123 avenue Albert Thomas - 87000, Limoges, France
simone.naldi@unilim.fr
vincent.neiger@unilim.fr

[2]UVSQ - Université de Versailles Saint-Quentin-en-Yvelines
55 avenue de Paris
78035 Versailles cedex, France
younessgrace@gmail.com

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Computing Recurrence Relations of $n-$dimensional Sequences Using Dual of Ideals

Angelos Mantzaflaris[1], **Hamid Rahkooy**[2], **Éric Schost**[2]

We consider the problem of computing the ideal of linear recurrence relations of a sequence over $\mathbb{N}^n$. We call this ideal the annihilator of the sequence. We restrict ourselves to the case that the annihilator is $\mathfrak{m}-$primary, which allows us to assume that the values of the sequence is zero outside a finite set $\mathcal{M}$, hence the input is the values over $\mathcal{M}$. Our algorithm can easily be generalized into arbitrary number of sequences whose annihilator is zero-dimensional.

Berlekamp and Massey considered the problem for sequences over $\mathbb{N}$ and gave an algorithm for it in 1960s [2, 7]. Sakata generalized the problem into the sequences over $\mathbb{N}^n$ [10]. In terms of Macaulay's *Inverse System* [5], the annihilator is the orthogonal of the inverse system of a given element. In other words, the problem is to find the ideal, for which the dual module is given. Marinari, Mora, Möller and Alonso introduced algorithms for this duality problem [1, 6], considering it as a generalization of FGLM [4].

A first approach to solve this problem is to consider a recurrence relation with symbolic coefficients and plug in the sequence in order to obtain linear equations. This leads to solving a Hankel matrix of size $s = |\mathcal{M}|$. Let d be the dimension of the quotient of the polynomial ring with the annihilator, as a vector space, and δ be the size of the border of the annihilator. Faugere, et. al. in [3] consider $\mathcal{M}$ to be the set of tuples $(a_1, \cdots, a_n)$, with $a_1 + \cdots + a_n \leq t$, for some $t \in \mathbb{N}$, and give an algorithm of complexity $O(s^\omega + \delta d^\omega)$, where ω is the constant in the complexity of matrix multiplication. In a recent work, Mourrain presented an algorithm —in a more general setting for computing border basis— with complexity $O(nd^2s)$ [8].

Motivated by Mourrain's *Integration Method* [9] for fast computation of the dual of an $\mathfrak{m}-$primary ideal, we convert the problem of computing the annihilator into the problem of finding the dual of a certain ideal. Unlike all other algorithms, our algorithm essentially looks for the linear dependencies among the values of the sequence, going from the largest tuple in $\mathcal{M}$ to the smaller ones. The complexity of our algorithm is $O\left(n(s-d)^3 + n(s-d)C + ns\right)$, where C is the cost of the integrations done during the integration method. We present classes of sequences for which $s-d$ is small while s and d are large enough, hence our algorithm is faster than all above algorithms. We have implemented our algorithm in Maple and our experiments show drastic reduction in the size of the matrices when $s-d$ is small.

Keywords: Linear recurrent sequences; Berlekamp-Massey Algorithm; Sakata's Problem; 0-dimensional ideal; n-dimensional sequences; dual of ideals.

References

[1] M. E. ALONSO; M. G. MARINARI; T. MORA, The big mother of all dualities 2: Macaulay bases. *Applicable Algebra in Engineering, Communication and Computing* **17**(6), 409–451 (2006).

[2] E. BERLEKAMP, Nonbinary bch decoding. *IEEE Transactions on Information Theory* **14**(2), 242–242 (1968).

[3] J. BERTHOMIEU; B. BOYER; J-C. FAUGÈRE, Linear algebra for computing gröbner bases of linear recursive multidimensional sequences. *ournal of Symbolic Computation* **83**(Supplement C) 36– 67 (2017).

[4] J. C. FAUGÈRE; P. GIANNI; D. LAZARD; T. MORA, Efficient computation of zero-dimensional gröbner bases by change of ordering. *Journal of Symbolic Computation* **16**(4), 329–344 (1993).

[5] F. S. MACAULAY, *The Algebraic Theory of Modular Systems*. Cambridge mathematical library. Cambridge University Press, Cambridge, New York, Melbourne, 1994.

[6] M. G. MARINARI; H. M. MÖLLER; T. MORA, Gröbner bases of ideals defined by functionals with an application to ideals of projective points. *Applicable Algebra in Engineering, Communication and Computing* **4**(2), 103–145 (1993).

[7] J. MASSEY, Shift-register synthesis and bch decoding. *IEEE Transactions on Information Theory* **15**(1), 122–127 (1969).

[8] B MOURRAIN, Fast algorithm for border bases of artinian gorenstein algebras. In *International Symposium on Symbolic and Algebraic Computation*, M. Burr (eds.), 333–340, ACM, New York, 2017.

[9] B. MOURRAIN Isolated points, duality and residues. *Journal of Pure and Applied Algebra* **117 & 118**, 469–493 (1997).

[10] S. SAKATA Extension of the Berlekamp-Massey algorithm to N dimensions. *Information and Computation* **84**(2), 207–239 (1990).

[1]Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences
Linz, Austria
angelos.mantzaflaris@oeaw.ac.at

[2]Cheriton School of Computer Science
University of Waterloo
Canada
hamid.rahkooy@uwaterloo.ca
eschost@uwaterloo.ca

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Special Properties of Zero-Dimensional Ideals: new Algorithms

Lorenzo Robbiano[1]

An affine 0-dimensional K-algebra is a ring of type P/I where K is a field, I is an ideal in $P = K[x_1, \ldots, x_n]$, and $\dim_K(P/I) < \infty$. In this talk some features of 0-dimensional affine K-algebras will be investigated: having the Cayley-Bacharach property, being locally Gorenstein, and being locally a complete interesection. In particular, the history of these properties and the modern approach via computational methods will be discussed.

Let us have a better look at the content of the presentation.

In book [2] we construct the theory of commuting families of endomorphisms of a finite dimensional K-vector space V, i.e., of families of endomorphisms of V which commute pairwise. In particular, we transfer the concept of commendability from a single endomorphism to a commuting family. It turns out that is strong enough for a fundamental theorem: a family is commendable if and only if V is a cyclic module with respect to the dual family. As abstract this may seem, it is the heart of some of the most powerful algorithms. The reason is that a zero-dimensional affine algebra R over a field K is identified with a commuting family via its multiplication family $\mathcal{F}$. This identification brings the extensive linear algebra preparations to fruition, and surprising connections between the two fields appear: the generalized eigenspaces of $\mathcal{F}$ are the local factors of R, the joint eigenvectors of $\mathcal{F}$ are the separators of R, there is a commendable endomorphism in $\mathcal{F}$ if and only if R is curvilinear, and the family $\mathcal{F}$ is commendable if and only if R is a *locally Gorenstein ring*. From this link a beautiful algorithm can be constructed which checks whether a zero-dimensional affine algebra is locally Gorenstein or not.

The notion of *complete intersection subscheme* is ubiquitous in Algebraic Geometry and Commutative Algebra where it takes the name of *ideal generated by a regular sequence*. Surprisingly, an old result by Wiebe (see [6]) can be successfully used to check whether an affine 0-dimensional local K-algebra is a complete intersection or not. And the full process is algorithmic.

The history of the *Cayley-Bacharach property (CBP)* goes back to Pappus Alexandrinus (ca. 320) and keeps going on. Some steps and turns will be illustrated. Recently, it became clear that, in order to study general versions of the CBP, it is preferable to formulate it as a property of the respective coordinate rings rather than sets of points or 0-dimensional schemes. In this vein, we defined in [2] the CBP for 0-dimensional affine algebras with a fixed presentation with arbitrary K and linear

maximal ideals, and provided several algorithms to check it. A couple of years ago the most general definition of the CBP to date was given by Long in [5] where he considered it for presentations of arbitrary 0-dimensional affine algebras over arbi-trary base fields. The definition in [5] and a clever use of the canonical module is the starting point of [3] where we study this very general version of the CBP and find efficient algorithms for checking it.

All the examples mentioned in the talk were computed with CoCoA (see [1]).

Keywords: Cayley-Bacharach, Gorenstein, canonical module, complete intersection

References

[1] J. Abbott, A.M. Bigatti, L. Robbiano, *CoCoA: a system for doing Computations in Commutative Algebra.* Available at `http://cocoa.dima.unige.it`

[2] M. Kreuzer, L. Robbiano, COMPUTATIONAL LINEAR AND COMMUTATIVE ALGEBRA,
Springer 2016

[3] M. Kreuzer, L. N. Long, L. Robbiano, *On the Cayley-Bacharach Property* Preprint (2017).

[4] M. Kreuzer, L. N. Long, L. Robbiano, *Subschemes of the Border Basis Scheme*, Preprint (2018)

[5] L.N. Long, Various differents for 0-dimensional schemes and appplications, dissertation, University of Passau, Passau, 2015.

[6] H. Wiebe, über homologische Invarianten lokaler Ringe, Math. Ann. **179** (1969), 257-274.

[1]Dipartimento di Matematica
Università di Genova
Via Dodecaneso 35, 16146 Genova
`lorobbiano@gmail.com`

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Signature-based Criteria for Computing Weak Gröbner Bases over PIDs

Thibaut Verron[1], **Maria Francis**[1]

The theory of Gröbner bases was introduced by Buchberger in 1965 [2] and has since become a fundamental algorithmic tool in computer algebra. Over the past decades, many algorithms have been developed to compute Gröbner bases more and more efficiently. The latest iteration of such algorithms is the class of signature-based algorithms, which introduce the notion of signatures and use it to detect and prevent unnecessary or redundant reductions. This technique was first introduced for Algorithm F5 [5], and there have been many research works in this direction [3].

All these algorithms are for ideals in polynomial rings over fields. Gröbner bases can be defined and computed over commutative rings [1, Ch. 4], and can be used in many applications [7]. An important particular case is that where the coefficient ring is a Principal Ideal Domain (PID), for example $\mathbb{Z}$ or the ring of univariate polynomials over a field.

If the coefficient ring is not a field, there are two ways to define Gröbner bases, namely weak and strong bases. Strong Gröbner bases ensure that normal forms can be computed as in the case of fields. But computing a strong Gröbner basis is more expensive than a weak one, and if the base ring is not a Principal Ideal Domain (PID), then some ideals exist which do not admit a strong Gröbner basis. On the other hand, weak Gröbner bases, or simply Gröbner bases, always exist for polynomial ideals over a Noetherian commutative ring. They do not necessarily define a unique normal form, but they can be used to decide ideal membership.

Recent works have focused on generalizing signature-based techniques to Gröbner basis algorithms over rings. First steps in this direction, adding signatures to a modified version of Buchberger's algorithm for strong Gröbner bases over Euclidean rings [6], were presented in [4]. The paper proves that a signature-based Buchberger's algorithm for strong Gröbner bases cannot ensure correctness of the result after encountering a "signature-drop", but can nonetheless be used as a prereduction step in order to significantly speed up the computations.

Here we consider the problem of computing a weak Gröbner basis of a polynomial ideal with coefficients in a PID, using signature-based techniques. The proof-of-concept algorithm that we present is adapted from that the general algorithm due to Möller [8], which considers combinations and reductions by multiple polynomials at once. The way the signatures are ordered ensures that no reductions leading to signature-drops can happen. In particular, we could prove that the algorithm terminates and computes a signature Gröbner basis with elements ordered with non-decreasing signatures. This property allows us to examine classic signature-based

criteria, such as the syzygy criterion, the F5 criterion and the singular criterion, and show how they can be adapted to the case of PIDs. In particular, when the input forms a regular sequence, the algorithm performs no reductions to zero.

We have written a toy implementation in Magma of the algorithms presented, with the F5 and singular criteria. Möller's algorithm, without signatures, works for polynomial systems over any Noetherian commutative ring. The signature-based algorithm is only proved to be correct and to terminate for PIDs, but with minimal changes, it can be made to accommodate inputs with coefficients in a more general ring. Interestingly, early experimental data with coefficients in a multivariate polynomial ring (a Unique Factorization Domain which is not a PID) suggest that the signature-based algorithm might work over more general rings than just PIDs.

Keywords: Gröbner bases, Signature-based algorithms, Principal Ideal Domains

References

[1] ADAMS, W. & LOUSTAUNAU, P. (1994). *An Introduction to Gröbner Bases*. American Mathematical Society.

[2] BUCHBERGER, B. (1965). *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. Ph.D. thesis, University of Innsbruck, Austria.

[3] EDER, C. & FAUGÈRE, J.-C. (2017). A Survey on Signature-based Algorithms for Computing Gröbner Bases. *Journal of Symbolic Computation* **80**, 719–784.

[4] EDER, C., PFISTER, G. & POPESCU, A. (2017). On Signature-Based Gröbner Bases over Euclidean Rings. In: *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '17. New York, NY, USA: ACM.

[5] FAUGÈRE, J. C. (2002). A New Efficient Algorithm for Computing GrÖbner Bases without Reduction to Zero (F5). In: *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, ISSAC '02. New York, NY, USA: ACM.

[6] LICHTBLAU, D. (2012). Effective Computation of Strong Gröbner Bases over Euclidean Domains. *Illinois J. Math.* **56**(1), 177–194 (2013).

[7] LICHTBLAU, D. (2013). Applications of Strong Gröbner Bases over Euclidean Domains. *Int. J. Algebra* **7**(5-8), 369–390.

[8] MÖLLER, H. M. (1988). On the Construction of Gröbner Bases using Syzygies. *Journal of Symbolic Computation* **6**(2-3), 345–359.

[1]Institute for Algebra
Johannes Kepler University
4040 Linz, Austria
thibaut.verron@jku.at
maria.francis@jku.at

S12

Numerical Differential and Polynomial Algebra

The aim of this session is bring together researchers and practitioners working with systems of polynomials and also those working with systems of polynomially nonlinear differential equations. A particular emphasis of our session is on approximate methods for such systems. There have been many recent developments which yield homotopy based methods for determining approximate points on solution components of such systems. The session will also encourage contributions on the much less developed area of approximate differential algebra, fundamentally important in applications to dynamical models. We invite participants in both theory and applications to this session. This session has an overlap with the session Computational Differential and Difference Algebra. Expected topics of presentations include (but are not limited to):

- Numerical Polynomial Algebra
- Approximate Differential Algebra
- Numerical homotopy methods for witness points of polynomial systems
- Approximate geometric involutive differential systems
- PDAE and DAE and their applications
- Numerical methods for approximate critical points of real polynomial systems

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Symbolic-numeric methods for simulation of cosserat rods

Dmitry Lyakhov [1]

We derive a combined analytical and numerical scheme to solve differential Kirchhoff system. Here the object is to obtain an accurate as well as an efficient solution process. Purely numerical algorithms typically have the disadvantage that the quality of the solutions decreases enormously with increasing temporal step sizes, which results from the numerical stiffness of the underlying partial differential equations. To prevent that, we apply a differential Thomas decomposition and a Lie symmetry analysis to derive explicit analytical solutions to specific parts of the Kirchhoff system. These solutions are general and depend on arbitrary functions, which we set up according to the numerical solution of the remaining parts. In contrast to a purely numerical handling, this reduces the numerical solution space and prevents the system from becoming unstable. The differential Kirchhoff equation describes the dynamic equilibrium of one-dimensional continua, i.e. slender structures like fibers. We evaluate the advantage of our method by simulating different scenarios, relevant in visual computing.

[1]King Abdullah University of Science and Technology
Thuwal, Saudi Arabia
dmitry.lyakhov@kaust.edu.sa

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

A symbolic-numeric method to determine symmetry of approximate differential equations

Zahra Mohammadi[1], **Greg Reid**[1]

We extended a critical point method based on penalty function introduced by Reid and Wu [1] to determining symmetry properties of general class of Differential Algebraic Equations DAE. This method interplay between geometric involutive form and numerical algebraic geometry which is based on homotopy methods.
There has been considerable progress on exploiting exact symmetry of exact system of DAE which using powerful symbolic packages such as ***rifsimp*** to get the involutive form of the system. These methods are less suited in applications since the coordinate dependency on ordering the variables can lead to numerical instability, especially on approximate systems. Our method applies a combination of geometric involutive form and critical point methods on the symmetry defining equations.
This work is sequel to [3] in which Numerical Linear Algebra is used to obtain an involutive of the system. In this work, we obtain useful information related all components of the involutive form of the DAE system and symmetry properties, by finding a witness points on each connected component. The approach exploits aspects of the termination of *Cartan- Kuranishi* theory of partial differential equations together with method of numerical algebraic geometry.

Keywords: Critical point, Numerical Algebraic Geometry, Symmetry.

References

[1] W.WU; C.CHANGBO AND G.REID, Penalty Function Based Critical Point Approach to Compute Real Witness Solution Points of Polynomial System *Computer Algebra in Scientific Computing*, 377-391, (CASC 2017).

[2] M. KURANISHI, On. E. Cartan's prolongation theorem of exterior differential systems. *Am. J. Math* **79**, 1-47 (1957).

[3] J.BONASIA; F.LEMAIRE; G.REID AND L.ZHI, Determination of approximate symmetries of differential equations. *Group Theory and Numerical Analysis*, 249-266 (2005).

[1]Applied Mathematics
Western University
Middlesex College,
1151 Richmond Street, London, Ontario
N6A 5B7 Canada
zmohamm5@uwo.ca
reid@uwo.ca

Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Challenges in Numerical Differential Algebra

Greg Reid[1], **Zahra Mohammadi**[1]

Much recent progress has been made in numerical polynomial algebra with the advent of homotopy-based methods and methods based on numerical linear algebra.

In this talk we review some of these developments, in the context of developing analogous methods for numerical differential algebra. A selecta of applications is given, including region dependent approximate symmetry, and determination of missing constraints in over and under-determined systems of partial differential equations with constraints. Geometric methods for such systems, together with stable methods form numerical linear algebra underly such approaches. Animations illustrating the application to approximate symmetries will be shown.

[1]Applied Mathematics
Western University
Middlesex College
1151 Richmond Street, London, Ontario
N6A 5B7 Canada
reid@uwo.ca
zmohamm5@uwo.ca

Index of authors

C U R S O S E C O N G R E S O S
Nº 248

USC
UNIVERSIDADE DE SANTIAGO DE COMPOSTELA