ACA 2021 Book of Abstracts

https://aca2021.sba-research.org/ July 23-27, 2021 (online)

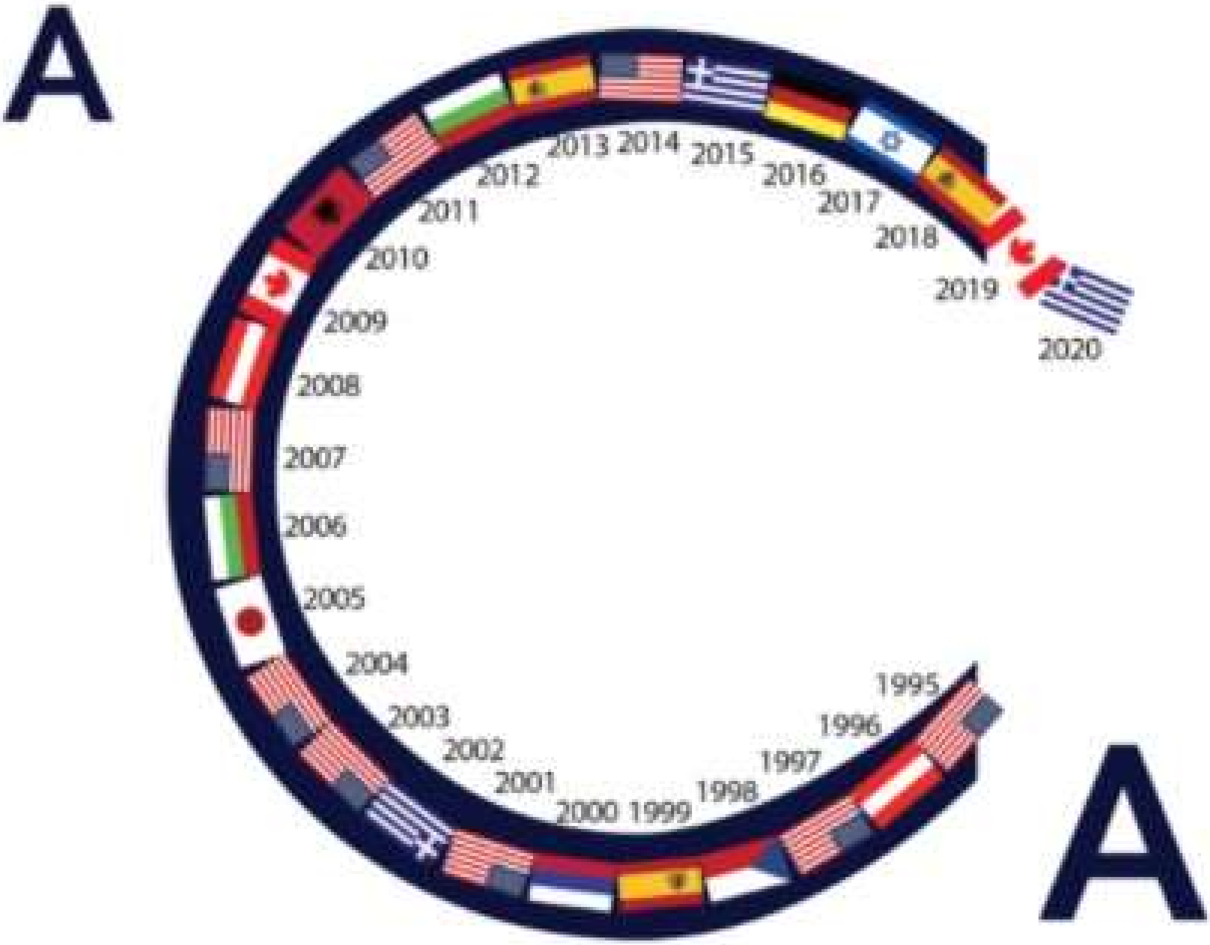
Bernhard Garn

Ludwig Kampel

Ilias Kotsireas

Dimitris Simos

Michael Wester



PREFACE

Welcome to the 26th conference on Applications of Computer Algebra (ACA'2021). Originally, this meeting was scheduled for 2020 in Athens, Greece, but due to the SARS-CoV-2/COVID-19 pandemic, we rescheduled the conference to 2021 and made it entirely virtual for this year. We are indebted to all the organizers and speakers who were able to reschedule their sessions to one year later than originally planned.

We would like to dedicate ACA'2021 to Vladimir Gerdt, who passed away from COVID-19 at the beginning of 2021. Vladimir was an ACA regular, and was frequently involved as a session organizer as well as program co-chair (ACA'1997 in Wailea, Maui, Hawaii and ACA'2004 in Beaumont, Texas) and general co-chair (ACA'2006 in Varna, Bulgaria and ACA'2008 at RISC-Linz, Austria). He was also a special guest to Albuquerque, New Mexico (where the ACA series originated in 1995) for ACA'2001.

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

We thank the generosity of the CARGO Lab and SBA Research MATRIS Research Group for taking care of the registration fee this year, using their own resources (and those offered by some of the session organizers) to make this virtual conference possible.
We also wish to express our thanks to Michel Beaudin, who instigated conversations on critical conference details.

We hope and expect that ACA'2022 will return to an in-person format. ACA is not simply a conference series, but a community of friends, and we will miss in-person interactions this year.
However, we will continue to have an excellent meeting with some 150+ half-hour presentation slots (a few talks are one hour) distributed amongst 13 sessions.

Thank you all very much for participating!

Michael J. Wester (co-general chair)
Ilias S. Kotsireas (co-general chair)
Dimitris E. Simos (program chair)

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Maple 2021"*

What's New in Maple 2021

Jürgen Gerhard[1] [jgerhard@maplesoft.com]

[1] Senior Director, Research, Maplesoft

We will give an overview of the new features of Maple 2021, including limits and asymptotic expansions, automatic plotting domain and range selection, a new Student:-ODEs package, approximate polynomial algebra, and improved LaTeX export.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Mathematica 12.3”*

New Calculus and Algebra Features in Mathematica 12.3

Devendra Kapadia[1] [dkapadia@wolfram.com]

[1] Wolfram Research, Inc.

The goal of this talk is to give an overview of the new functions and features related to Calculus and Algebra in Mathematica 12.3. I will begin by describing the support for solving systems of transcendental equations and the breakthroughs in exact and parametric optimization in Version 12.3. Next, an account will be given of the new functionality for computing bilateral Laplace transforms, the Ore reduction algorithm for solving systems of linear ordinary differential equations with rational coefficients, and the extensive monograph on symbolic solutions of partial differential equations that is available in the latest release. Finally, a brief introduction to the new Fox H-function and Carlson elliptic integral functions along with their applications will be given. I will conclude the talk by outlining recent initiatives related to function documentation and the development of free, interactive online courses at high school and college level in Calculus and Algebra.

Keywords
Mathematica, transcendental equations, exact optimization, parametric optimization, bilateral Laplace transform, Ore algebra, partial differential equations, Fox H-function, Carlson elliptic integrals, online education

References

[1] S. WOLFRAM, *Launching Version 12.3 of Wolfram Language & Mathematica*, https://blog.wolfram.com/2021/05/20/launching-version-12-3-of-wolfram-language-mathematica/.
[2] WOLFRAM, Summary of new features in 12.3, https://reference.wolfram.com/language/guide/SummaryOfNewFeaturesIn123

Dedication to Vladimir P. Gerdt

Prof. Vladimir P. Gerdt passed away in early January 2021.

Vladimir was the head of the Group of Algebraic and Quantum Computation at the Joint Institute for Nuclear Research, Dubna, Russia.

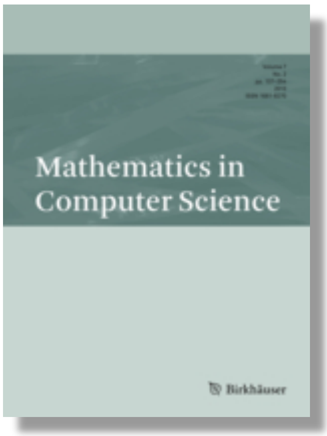
He was well known for his contributions to various aspects of symbolic and algebraic computation, related to nonlinear differential equations and polynomial systems, their exact and numerical solutions, their symmetries, and their applications to physics, quantum computation, etc. He initiated the theory of involutive bases (such as Janet bases and Pommaret bases), revived the method of Thomas decomposition for algebraic and differential systems, and developed many of their applications. His scientific works include more than 200 publications, and he was editor of the Journal of Symbolic Computation.

Vladimir was a regular contributor to *Applications of Computer Algebra*, e.g. through organizing a series of sessions on computational differential and difference algebra. Moreover, he was co-founder (with Ernst W. Mayr) of the *Computer Algebra in Scientific Computing* conference series.

We will miss him greatly.

MATHEMATICS IN COMPUTER SCIENCE
SPECIAL ISSUE in honor of Vladimir Gerdt

Call for Papers



Guest Editors

Daniel Robertz
University of Plymouth, UK
daniel.robertz@plymouth.ac.uk
Werner M. Seiler
University of Kassel, Germany
seiler@mathematik.uni-kassel.de

Important Dates

Submission deadline: September 30, 2021
Author notification: January 31, 2022
Camera ready: March 31, 2022

With great sadness have we learned that Vladimir P. Gerdt passed away in early January 2021. He was well known for his contributions to various aspects of symbolic and algebraic computation, related to nonlinear differential equations and polynomial systems, their exact and numerical solutions, their symmetries, and their applications to physics, quantum computation, etc. He initiated the theory of involutive bases (such as Janet bases and Pommaret bases), revived the method of Thomas decomposition for algebraic and differential systems, and developed many of their applications.

In honor and memory of Vladimir P. Gerdt, this Special Issue of Mathematics in Computer Science welcomes the following kinds of contributions, related to his work:

- *short memory notes (at most two pages),*
- *survey articles,*
- *original research papers.*

Survey articles and original research papers generally should not exceed 25 pages.
Expressions of interest for writing survey articles are invited by the editors at an early stage for coordination purposes.

Paper Submission

Papers should be submitted via EasyChair: https://easychair.org/conferences/?conf=gerdt21 . Please upload a pdf file for each submission. The final version should be prepared using LaTeX with the class file birkjour.cls. Instructions for authors may be found at https://www.springer.com/journal/11786/submission-guidelines .

S1. Algebraic Geometry from an Algorithmic Point of View

Organized by

Cristina Bertone and Francesca Cioffi

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic Geometry from an algorithmic point of view”*

Simplification of λ-ring expressions in the Grothendieck ring of Chow motives

David Alfaya[1,2] [dalfaya@comillas.edu]

[1] Department of Applied Mathematics, ICAI School of Engineering, Comillas Pontifical University, Madrid, Spain
[2] Institute for Research in Technology, ICAI School of Engineering, Comillas Pontifical University, Madrid, Spain

Let R be a ring. A λ-ring structure on R is set of maps (not necessarily homomorphisms) $\lambda^i : R \longrightarrow R$ for each $i \in \mathbb{N}$ which satisfy the following properties.

1. For all $x \in R$, $\lambda^0(x) = 1$ and $\lambda^1(x) = x$.
2. For all $x, y \in R$ and all $n \in \mathbb{N}$
$$\lambda^n(x+y) = \sum_{i=0}^{n} \lambda^i(x)\lambda^{n-i}(y)$$

A λ-ring is special if, moreover, for all $x, y \in R$ and all $n, m \in \mathbb{N}$

$$\lambda^n(xy) = P_n\left(\lambda^1(x), \ldots, \lambda^n(x), \lambda^1(y), \ldots, \lambda^n(y)\right)$$
$$\lambda^n(\lambda^m(x)) = P_{n,m}\left(\lambda^1(x), \ldots, \lambda^{nm}(x)\right)$$

where $P_n \in \mathbb{Z}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ and $P_{n,m} \in \mathbb{Z}[X_1, \ldots, X_{nm}]$ are certain universal polynomials called Grothendieck polynomials. Special λ-rings are endowed with a set of λ-ring homomorphisms ψ^n for each $n \in \mathbb{N}$ called Adams operations which arise as certain algebraic combinations of the special λ-structure.

On the other hand, given a λ-ring structure λ on R, an “opposite” λ-ring structure σ can be defined by taking

$$\sum_{i \geq 0} \sigma^i(x)t^i = \left(\sum_{i \geq 0} \lambda^i(x)(-t)^i\right)^{-1}$$

Suppose that (R, λ) is a torsion free λ-ring such that its opposite λ-ring structure, σ, is special. By using algebraic relations between the λ-ring structures and the Adams operations, in this work, I present algorithms which perform an effective symbolic simplification of arbitrary algebraic expressions involving any combinations of the λ-ring structures and the Adams operations.

From the algebraic geometry point of view, one important example of a λ-ring whose opposite λ-structure is special is given by $K(CM_{\mathbb{K}})$, the Grothendieck ring of effective Chow motives over a field $\mathbb{K}$ with rational coefficients. This ring admits a natural λ-ring structure induced by the symmetric product of varieties, given by

$$\lambda^i([Y]) = [\mathrm{Sym}^i(Y)]$$

for every algebraic variety Y over $\mathbb{K}$. As described before, starting from this structure λ, an opposite λ-ring structure σ can be defined on $K(CM_{\mathbb{K}})$, and in [1] (also [2, §8]), it is proved that σ, contrary to λ, is a special structure. This property is also extended to some of its most commonly used localizations and completions with respect to the Lefschetz motive $\mathbb{L} = [\mathbb{A}^1]$, such as $K(CM_{\mathbb{K}})[\mathbb{L}^{-1}]$ and its dimensional completion $\hat{K}(CM_{\mathbb{K}})$.

These two λ-structures (specially the first one) arise naturally during the computation of the motivic classes of many different types of moduli spaces. For instance, if X is a smooth complex projective curve, the motives in the completion $\hat{K}(CM_{\mathbb{C}})$ of the Jacobian of X, the moduli space of vector bundles on X [3] or the moduli space of Higgs bundles on X [4, 5, 6, 7] can all be described as certain algebraic expressions in the sub-λ-ring of $\hat{K}(CM_{\mathbb{C}})$ generated by the curve X. Nevertheless, manipulating and simplifying the resulting expressions can become hard, usually due to a combinatorial explosion.

The proposed methodology allows the symbolic simplification of algebraic expressions in the sub-λ-ring of motives generated by a finite set of curves, transforming any such algebraic expression into an integral polynomial in a small set of motivic generators.

More precisely, let $X_1, \ldots, X_n$ be a finite set of projective curves of genus $g_1, \ldots, g_n$ respectively. For all $[M] \in \hat{K}(CM_{\mathbb{K}})$ (or $K(CM_{\mathbb{K}})$) belonging to the sub-(λ, σ)-ring generated by $X_1, \ldots, X_n$ there exists a polynomial

$$P_{[M]} \in \mathbb{Z}[l, \lambda_{1,1}, \ldots, \lambda_{1,g_1}, \lambda_{2,1}, \ldots, \lambda_{n,g_n}]$$

such that

$$[M] = P_{[M]}(\mathbb{L}, \lambda^1(h^1(X_1)), \ldots, \lambda^{g_1}(h^1(X_1)), \lambda^1(h^1(X_2)), \ldots, \lambda^{g_n}(h^1(X_n)))$$

where $\mathbb{L} = [\mathbb{A}^1]$ is the Lefschetz motive and $h^1(X) = [X] - 1 - \mathbb{L}$. Given an algebraic expression for $[M]$, the proposed algorithms find the polynomial $P_{[M]}$.

As an application, using the formulas from [8], the motives, E-polynomials and Betti numbers of some moduli spaces of Lie algebroid connections are explicitly computed in $\hat{K}(CM_{\mathbb{C}})$, and it is verified that the resulting E-polynomials and Betti numbers agree with the results of [5] and [6] on the moduli space of twisted Higgs bundles.

Moreover, using the proposed algorithm it is shown that the conjectural formula for the motive of the moduli space of twisted Higgs bundles given by Mozgovoy [6,7] agrees with the formula for the motive of the moduli space of Lie algebroid conections proven in [8], thus verifying the conjecture in low rank, genus and degree.

Keywords
λ-rings, symbolic computation of motives, moduli spaces

References

[1] F. HEINLOTH, A note on functional equations for zeta functions with values in Chow motives. *Ann. Inst. Fourier* **57**(6), 1927–1945 (2007).

[2] M. LARSEN; V. A. LUNTS, Rationality criteria for motivic zeta functions. *Compositio Mathematica* **140**(6), 1537–1560 (2004).

[3] K. BEHREND; A. DHILLON, On the motivic class of the stack of bundles. *Adv. in Math* **212**, 617–644 (2007).

[4] O. GARCÍA-PRADA; J. HEINLOTH; A. SCHMITT, On the motives of moduli of chains and Higgs bundles. *Journal of the European Mathematical Society* **16**, 2617–2668 (2014).

[5] W-Y. CHUANG; D-E. DIACONESCU; G. PAN, Wallcrossing and cohomology of the moduli space of Hitchin pairs. *Commun. Number Theory Phys* **5**(1), 1–56 (2011).

[6] S. MOZGOVOY, Solutions of the motivic ADHM recursion formula. *Int. Math. Res. Not.* **2012**(18), 4218–4244 (2012).

[7] S. MOZGOVOY; R. O'GORMAN, Counting twisted Higgs bundles. *arXiv:1901.02439* (2019).

[8] D. ALFAYA; A. OLIVEIRA, Lie algebroid connections, twisted Higgs bundles and motives of moduli spaces. *arXiv:2102.12246* (2021).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic Geometry from an algorithmic point of view”*

Fundamental groups in classification of algebraic surfaces

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

[1] Mathematics Department, SCE, Israel

The classification of algebraic surfaces in the moduli space has been an interesting question for many years. Some works were done in this research domain, for example for surfaces with Zappatic singularities, degree 6 surfaces, and surfaces that degenerate to non-planar shapes. We consider an algebraic surface X in some projective space. We project X onto the projective plane $\mathbb{CP}^2$, using a generic projection, and get the branch curve S in $\mathbb{CP}^2$. The curve S is a cuspidal curve with nodes and branch points, and it can tell a lot about X, but it is difficult to describe it explicitly. To tackle this problem, we use a nice degeneration and regeneration algorithm, that enables us to split S into local pieces and singularities.

Using the braid monodromy technique of Moishezon-Teicher [3] and van Kampen Theorem [4], we calculate the fundamental group G of the complement of S. Group G does not change when the complex structure of X changes continuously. In fact, all surfaces in the same component of the moduli space have the same homotopy type and therefore have the same group G. Then we calculate a special quotient of G, which is the fundamental group G_{Gal} of the Galois cover of X, and this quotient does not change when the complex structure of X changes continuously.

Here are examples and results on G_{Gal}: In [1] we prove that surfaces with Zappatic singularity of type R_k have a trivial G_{Gal}. And in [2] we divide surfaces with degree 6 degenerations to two sets: trivial or non-trivial G_{Gal}. During the talk, my student Mo, supervised jointly by me and Gong, will speak few minutes on the work [1].

In the end of the talk I will present an output of a new computer algorithm, developed jointly with Uriel Sinichkin (Tel-Aviv University, Israel), which gives braids of S and relations of G.

Keywords
classification of surfaces, fundamental groups

References

[1] AMRAM, M., GONG, C., MO, J.-L., On the Galois covers of degenerations of surfaces

of minimal degree (2021).

[2] AMRAM, M., GONG, C., SINICHKIN, U., TAN, S.-L., XU, W.-Y., YOSHPE, M., Fundamental groups of Galois covers of degree 6 surfaces, arXiv:2012.03279 (2020).

[3] MOISHEZON B., TEICHER, M., Braid group technique in complex geometry II, From arrangements of lines and conics to cuspidal curves. *Algebraic Geometry, Lect. Notes in Math.* **1479**, 131–180 (1991).

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

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic Geometry from an Algorithmic Point of View”*

Waring decompositions of real binary forms and Brion’s formula

M. Ansola[1]***, A. Diaz-Cano***[2]***, M. A. Zurro***[3] [mansola@ucm.es]

[1] Algebra, Geometry and Topology Department, Universidad Complutense, Madrid, Spain
[2] Algebra, Geometry and Topology Department & Interdisciplinary Mathematics Institute (IMI), Universidad Complutense, Madrid, Spain
[3] Mathematics Department, Universidad Autónoma de Madrid, Madrid, Spain

The Waring Problem over polynomial rings studies the decomposition of a homogeneous polynomial p of degree d in n variables as a linear combination of d-th powers of linear forms with coefficients in a field K. Such an expression of p is called a *Waring decomposition* (WD) of that form and when we take r minimal with this property, we call r *the Waring rank* of p over K.

This type of decompositions has many applications in Mathematics, Engineering, Physics (see [8], [9] and the many references therein) and even areas of such recent development as Data Mining or Machine Learning (see the numerous references in the introduction of [4]).

We study the case $K = \mathbb{R}$ and $n = 2$. The real case is especially interesting for the applications (see [3]). This real case has been extensively investigated by different authors (for instance, in [8], [10] or [11]). It is also known that the complex Waring rank is less than or equal to the real Waring rank (see [3]). For example, consider

$$p(x, y) = -y^3 - 3xy^2 + 3x^2y + x^3.$$

Then, there is an essentially unique WD of length 2 with complex coefficientes: $p(x, y) = \left(\frac{1}{2} - \frac{i}{2}\right)(x+i\,y)^3 + \left(\frac{1}{2} + \frac{i}{2}\right)(x-i\,y)^3$. However, it can be shown that if we require a WD to have real coefficients, then 3 real linear forms will be needed, because of Sylvester Algorithm in the real case, see [12], [9]. In fact, for any real number $s \neq 0, \pm 1$, we have

$$p(x, y) = -\frac{1}{s(s-1)}(x + sy)^3 - \frac{1}{s(s+1)}(x - sy)^3 + \frac{s^2+1}{s^2-1}(x + y)^3.$$

Presenting these types of problems from an algorithmic point of view is very different when considering complex coefficients or real coefficients. In the complex case, the algorithms published in [5] and [6] provide a fairly fast probabilistic algorithm for generic complex binary forms. In the real case, a deterministic algorithm can be given to calculate a Waring decomposition of a real binary form p of length at most its degree. As far as we know, our work ([1]) is the first algorithm that provides an optimal WD decomposition for the monomials, since their real rank is d, see [8]. First, we will present this algorithm in the talk.

In [2], Baldoni et al. considered the problem of how to efficiently compute the exact value of the integral of a polynomial $f \in \mathbb{Q}[x_1, \dots, x_n]$ over a d-dimensional simplex Δ in $\mathbb{R}^n$. The measure considered was the integral Lebesgue measure, that we will denote by dm and the integral we want to compute by $\int_\Delta f\, dm$. One of the methods to compute the above integral is by means of a WD of the polynomial f. Then, the essential problem is to compute the d-th power of any linear form on the simplex Δ. With this approach, in 2010, the following result was established.

Theorem (Brion's formula, [2]) Let Δ be the simplex, that is the convex hull of $\nu+1$ affinely independent vertices $s_1, \dots s_{\nu+1}$ in $\mathbb{R}^n$, $\ell = \sum_{k=1}^n a_k x_k$ a real linear form, and d a positive integer. Then we have:

$$\sum_{d\in\mathbb{N}} T^d \frac{(d+\nu)!}{d!} \int_\Delta \ell^d dm = \nu! \, \mathtt{vol}(\Delta, dm) \frac{1}{\prod_{j=1}^{\nu+1} (1 - T < \ell, s_j >)}, \qquad (1)$$

with T a variable over $\mathbb{R}$, and $< \ell, s_j > := \sum_{k=1}^n a_k s_{j,k}$ for $s_j = (s_{j,1}, \dots, s_{j,n})$.

It should be noted that achieving an effective real decomposition of minimum length is the ultimate goal of this approach to integration of polynomials over simplices using the evaluation formula at its vertices.

In the last part of the talk, we will show how to **effectively compute** integrals of polynomials over a finite triangulation by means of our algorithm (see [1]) to compute Waring decompositions. Also a parametric version of formula (1) will be presented. The techniques are based on the study of families of semialgebraic sets associated with p, the given real binary form. Some examples computed with Maple will be shown.

Keywords
Real algebraic sets, Real binary forms, Waring decompositions, Brion's formula.

Acknowledgements
The second and third authors acknowledge the support of Grupo UCM 910444.

References

[1] M. ANSOLA; A. DÍAZ-CANO; M.A. ZURRO, Semialgebraic sets and real binary forms decompositions. *J. Symbolic Comput.* **107**, 209–220 (2021).

[2] V. BALDONI; N. BERLINE; J. DE LOERA; M. KÖPPE; M. VERGNE, How to integrate a polynomial over a simplex. *Math. Comp.* **80**, 297–325 (2011).

[3] E. BALLICO; A. BERNARDI, Real and complex rank for real symmetric tensors with low ranks. *Algebra, Hindawi Publishing Corporation* **2013**, Article ID 794054 (2013).

[4] B.W. BADER; T.G. KOLDA, Tensor Decompositions and Applications. *SIAM Rev.* **51**, 455–500 (2009).

[5] M.R. BENDER; J.C. FAUGÈRE; L. PERRET; E. TSIGARIDAS, A Superfast Randomized Algorithm to Decompose Binary Forms. *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC '16, ACM*, 79–86. New York (2016).

[6] M.R. BENDER; J.C. FAUGÈRE; L. PERRET; E. TSIGARIDAS, A nearly optimal algorithm to decompose binary forms. *J. Symbolic Comput.* **105**, 71–96 (2021).

[7] A. BERNARDI; I. CARUSOTTO, Algebraic Geometry tools for the study of entanglement: an application to spin squeezed states. *J. Phys. A* **45**, 105304 (2012).

[8] M. BOIJ; E. CARLINI; A.V. GERAMITA, Monomials as sums of powers: the real binary case. *Proc. Amer. Math. Soc.* **139**, 3039–3043 (2011).

[9] J. BRACHAT; P. COMON; B. MOURRAIN; E. TSIGARIDAS, Symmetric tensor decomposition. *Linear Algebra Appl.* **433**, 1851–1872 (2010).

[10] P. COMON; G. OTTAVIANI, On the typical rank of real binary forms. *Linear Multilinear Algebra* **60**, 657–667 (2012).

[11] B. REZNICK, Laws of inertia in higher degree binary forms. In *Proc. Amer. Math. Soc.* **138**, 815–826 (2010).

[12] J.J. SYLVESTER, Sur une extension d'un théorème de Clebsch relatif aux courbes du quatrième degré. In *C. R. Math. Acad. Sci. Paris* **102**, 1532–1534 (1886).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic Geometry from an algorithmic point of view”*

How to cover rational surfaces with few rational parametrization images

Jorge Caravantes[1]***, J. Rafael Sendra***[1]***, David Sevilla***[2]***, Carlos Villarino***[1] [jorge.caravantes@uah.es]

[1] Universidad de Alcalá, Dpto. Física y Matemáticas, Alcalá de Henares, Madrid, Spain
[2] Universidad de Extremadura, Dpto. de Matemáticas, Mérida, Badajoz, Spain

Rational varieties (in particular curves and surfaces) play an important role in many geometric applications like those in computer aided design [1] or computer vision [2]. This is to a large extent due to having both implicit and parametric representations. For certain computations it is important that the parametric representation has certain properties, like injectivity or surjectivity. The case of curves is well understood [3]. For the case of surfaces, we present here some results relative to two aspects: the existence of surjective *birational* (i.e. generically injective) parametrizations, and the existence of small *coverings* of parametric rational surfaces, that is, collections of a few rational parametrizations such that the union of their images cover the given surface.

It is important, first, to clarify the setting of our results. In general, they are valid for surfaces over the algebraically closed fields of characteristic zero, like $\mathbb{C}$ or $\overline{\mathbb{Q}}$. Another caveat is that in geometric settings it is usual to work in *affine* spaces but some important results in algebraic geometry work for varieties in *projective* spaces.

This talk presents the main results of [4] and [5], and also some future work in this direction

1 Parametrizability with birational maps

Our first result is a necessary condition on an affine rational map to be extensible to a projective birational map.

Theorem (Theorem 3.1 in [4]). *Let $f : \mathbb{C}^2 \dashrightarrow \mathbb{C}^N$ be a rational map. Let S be the Zariski closure of $f(\mathbb{C}^2)$ in $\mathbb{C}^N$, and suppose that f is birational and surjective onto S. Let $\overline{S}$ be the Zariski closure of S in $\mathbb{P}^N$ and $S_\infty = \overline{S} - S$ the hyperplane section at infinity.*

If $\overline{S}$ is smooth, then S_∞ has at least $\rho(\overline{S})$ rational components, where $\rho(\overline{S})$ is the Picard number (i.e. rank of the Picard group) of S.

Example (Example 4.2 in [4]). *Let S to be a smooth cubic surface. It is well known that $\overline{S}$ is isomorphic to $\mathbb{P}^2$ blown up at 6 general points. Then $\rho(\overline{S}) = 7$. On the other side, due to the degree, S_∞ has at most three components. Thus it is impossible to give a birational surjective parametrization of S, or more generally of the complement in $\overline{S}$ of any hyperplane section.*

2 Projective covering

This section and the next contain our covering algorithms. Let $S \subset \mathbb{P}^n$ be a rational projective surface and let

$$F = (F_0 : \cdots : F_n) : \mathbb{P}^2 \dashrightarrow \mathbb{P}^n$$

be a (not necessarily birational) parametrization of S, given by $n+1$ homogeneous coprime polynomials $F_0, \ldots, F_n$ where the nonzero polynomials have degree d. Let the homogeneous ideal $I = (F_0, ..., F_n)\mathbb{K}[x_0, x_1, x_2]$ be called the fundamental ideal associated to F. The points where I vanishes are called *base points of* F. If F has no base points, then it is a regular map, and its image is S; therefore, the restrictions of F to the affine planes $x_i \neq 0$, $i = 0, 1, 2$ cover S and its affine part. Let us assume then that the set of base points is nonempty and denote it as $\mathcal{A} := \{P_1, \ldots, P_k\}$.

The algorithm that will be described next is applicable to parametrizations satisfying the following mild assumptions:

- $(*)$ For every P_i the Jacobian matrix of F at P_i has rank 2.
- (a) no P_j is in any of the lines $\{x_0 = 0\}$, $\{x_1 = 0\}$ and $\{x_2 = 0\}$,
- (b) no pair $\{P_i,\ P_j\}$, $i \neq j$, is aligned with any of the coordinate points $(1:0:0)$, $(0:1:0)$ and $(0:0:1)$.

Note that (a) and (b) can be assumed without loss of generality since they are achievable from any given F by a change of coordinates.

Theorem. *Every projective surface with a parametrization satisfying $(*)$, (a) and (b) can be fully covered with three parametrizations (one of which is the given one). Furthermore, if the initial parametrization is birational, so are the other two.*

Proof. An algorithm to compute the covering parametrizations is given in [5]. □

In the talk, the computations will be shown for the case of the example of the previous section.

3 Affine covering

We consider now the problem of covering a rational affine surface by means of the images of several affine parametrizations. We prove that to cover a rational affine surface, only two patches are necessary.

Theorem. *Every affine surface with a parametrization satisfying* $(*)$, (a) *and* (b) *can be fully covered with two parametrizations (one of which is the given one). Furthermore, if the initial parametrization is birational, so is the other one.*

Proof. An algorithm to compute the covering parametrizations is also given in [5]. □

In the talk, the computations will be shown for the case of the example of the first section.

Keywords
Rational surface, Birational parametrization, Surjective parametrization, Surface cover, Base points

Acknowledgements
The authors are partially supported by FEDER/Ministerio de Ciencia, Innovación y Universidades - Agencia Estatal de Investigación/MTM2017-88796-P (Symbolic Computation: new challenges in Algebra and Geometry together with its applications).

The first, second and fourth authors are members of the Research Group ASYNACS (Ref. CT-CE2019/683). In addition, the second author is also partially supported by Dirección General de Investigación e Innovación, Consejera de Educación e Investigación of the Comunidad de Madrid (Spain), and Universidad de Alcalá (UAH) under grantCM/JIN/2019-010.The third author is a member of the research group GADAC and is partially sup-ported by Junta de Extremadura and FEDER funds (group FQM024)

References

[1] J. Hoschek; D. Lasser, *Fundamentals of computer aided geometric design.* A K Peters, Ltd., Wellesley, MA, 1993.

[2] M. K. Agoston, *Computer graphics and geometric modeling. Implementation and algorithms*, Springer, Berlin, 2005.

[3] J. R. Sendra; F. Winkler; S. Pérez-Díaz, *Rational algebraic curves*, volume 22 of *Algorithms and Computation in Mathematics*. Springer, Berlin, 2008.

[4] J. Caravantes; J. R. Sendra; D. Sevilla; C. Villarino, On the existence of birational surjective parametrizations of affine surfaces. *Journal of Algebra* **501**, 206–214 (2018). DOI: 10.1016/j.jalgebra.2017.12.028

[5] J. Caravantes; J. R. Sendra; D. Sevilla; C. Villarino, Covering rational surfaces with rational parametrization images. *Mathematics* **9**(4), 338 (2021).
DOI: 10.3390/math9040338

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic Geometry from an algorithmic point of view”*

Secret sharing schemes from hypersurfaces over finite fields

Angela Aguglia[1] ***Michela Ceria***[1]**, *Luca Giuzzi***[2] [michela.ceria@poliba.it]

[1] Dipartimento di Meccanica, Matematica e Management, Politecnico di Bari, Via Orabona 4, I-70125 Bari, Italy
[2] DICATAM, University of Brescia, Via Branze 53, I-25123 Brescia, Italy

A *secret sharing scheme* is a cryptographic procedure allowing to handle the access to a secret by a group of people, the participants. Every participant has a share of the secret and the whole secret can be retrieved only when a suitable group of participants puts its shares together.
Such a “suitable group of participants" is called *access set*, while the collection containing all access sets is called *access structure* for the given scheme.
We also say that an access set is *minimal*, if removing from it any participant, it is not possible to find out the secret anymore.

Massey, in [3], showed how linear error-correcting codes can be used to build secret sharing schemes, in particular showing the link between the access structures and the minimal words of the dual code.

In particular, the idea is that, taken a generator matrix G for the code, a trusted party considers a vector $\mathbf{u}$ and computes the product $\mathbf{u}G = (t_0, ..., t_{n-1})$; the first entry of this vector is the secret, while the other entries are the shares, which are distributed. A subset of shares $\{t_{i_1}, ..., t_{i_m}\}$ can reconstruct the secret if and only if there is a codeword $\mathbf{c} = (1, 0, ..., 0, c_{i_1}, 0, ..., c_{i_m}, 0, ..., 0)$ in the dual code, such that $c_{i_j} \neq 0$ for some j. A minimal codeword then gives rise to a minimal access set.

It is quite difficult to find out all minimal words in an arbitrary linear code and this difficulty translates in the difficulty in finding good access structures. Such structures are good since they are *democratic*, so every participant belongs to the same number of minimal access sets.

Let us consider the case of projective codes. Such codes are given by a generator matrix which has - as columns - the (properly normalized) coordinates of a collection of points in the finite projective space PG(r, q) of dimension r over the finite field $GF(q)$. For these codes some criteria for minimal words can be found.

In this talk we will consider as points, those of some hypersurfaces of PG(r, q^2), with $r \geq 3$ which appear in the construction of quasi-Hermitian varieties (see [1]) and such that their intersection numbers, with respect to hyperplanes, have only a few values. In particular, what we get is a code with five weights, corresponding to the five values of the intersection numbers.

We then study the weights of the associated projective codes and we will see that they are multiples of q except for a special case, namely $r = 3$ and q odd.

In the case of q odd, we will show the minimality of the codes and then that the associated secret sharing schemes have efficient access structures.

The talk refers to the preprint [2].

Keywords
Secret sharing scheme, minimal codewords, intersection numbers.

References

[1] A. AGUGLIA, A. COSSIDENTE, G. KORCHMÁROS, On quasi-Hermitian varieties *J. Comb. Designs* 20, 433–447 (2012).

[2] A. AGUGLIA, M. CERIA, L. GIUZZI, Secret sharing schemes from hypersurfaces over finite fields arXiv:2105.14508v2 [cs.IT]

[3] J.L. MASSEY, Minimal Codewords and Secret Sharing, *Proc. 6th Joint Swedish-Russian Workshop on Information Theory*, August 22-27, 276–279 (1993).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic Geometry from an algorithmic point of view”*

A characteristic free approach to secant varieties of triple Segre products

Aldo Conca[1]***, Emanuela De Negri***[1]***, Željka Stojanac*** [2] [denegri@dima.unige.it]

[1] Università di Genova, Genova, Italy
[2] Institute for Theoretical Physics, University of Cologne, Germany

In this talk I present some of the results obtained in [1] on the secant varieties of the triple Segre product of $\mathbb{P}^1 \times \mathbb{P}^{a-1} \times \mathbb{P}^{b-1}$. We work with 3-tensors of size $(2, a, b)$ with $2 \leq a \leq b$ and first consider the variety of rank-1 tensors, denoted by $\operatorname{Seg}(2, a, b)$. This corresponds to the image of the Segre embedding of $\mathbb{P}^1 \times \mathbb{P}^{a-1} \times \mathbb{P}^{b-1}$ in $\mathbb{P}^{2ab-1}$. For every $n \in \mathbb{N}$ denote by $[n]$ the set $\{1, 2, \dots, n\} \subset \mathbb{N}$. Recall that $\operatorname{Seg}(2, a, b)$ is a well understood toric variety. Equipping $[2] \times [a] \times [b]$ with the natural structure of distributive lattice one has that the defining ideal of $\operatorname{Seg}(2, a, b)$ in $R = K[x_{ijk} : (i, j, k) \in [2] \times [a] \times [b]]$ is

$$I(a, b) = (x_\alpha x_\beta - x_{\alpha\wedge\beta} x_{\alpha\vee\beta} : \alpha, \beta \text{ are incomparable elements of } [2] \times [a] \times [b]),$$

that is, the Hibi ideal of $[2] \times [a] \times [b]$ (see [3] for more informations on Hibi relations and Hibi ideals).

We also consider the t-secant variety $\sigma_t(2, a, b)$ of $\operatorname{Seg}(2, a, b)$, that is, the variety of rank-t tensors. Our main result is that the ideal $I(a, b)^{\{t\}}$ defining the secant variety $\sigma_t(2, a, b)$ is generated by determinantal equations coming from “unfoldings" of the associated tensors and that it defines a Cohen-Macaulay ring.

The *unfolding* is a transformation that reorganizes a tensor into a matrix. For a tensor $\mathcal{X}$ of size $n_1 \times n_2 \cdots \times n_d$, the k-th unfolding $\mathcal{X}^{\{k\}}$ is a matrix of size $n_k \times (n_1 \cdots n_{k-1} n_{k+1} \cdots n_d)$. The rows are indexed by the k-th index, and the columns are indexed by the vectors of the remaining indices. The order on the row and column indices is not important.

For example if $\mathcal{X} = (x_{ijk})$ is an order-3 tensor of size $2 \times 3 \times 3$, then, the first, second, and third unfolding are of the form

$$\mathcal{X}^{\{1\}} = \begin{bmatrix} x_{111} & x_{112} & x_{113} & x_{121} & x_{122} & x_{123} & x_{131} & x_{132} & x_{133} \\ x_{211} & x_{212} & x_{213} & x_{221} & x_{222} & x_{223} & x_{231} & x_{232} & x_{233} \end{bmatrix}$$

$$\mathcal{X}^{\{2\}} = \begin{bmatrix} x_{111} & x_{112} & x_{113} & x_{211} & x_{212} & x_{213} \\ x_{121} & x_{122} & x_{123} & x_{221} & x_{222} & x_{223} \\ x_{131} & x_{132} & x_{133} & x_{231} & x_{232} & x_{233} \end{bmatrix}$$

$$\mathcal{X}^{\{3\}} = \begin{bmatrix} x_{111} & x_{121} & x_{131} & x_{211} & x_{221} & x_{231} \\ x_{112} & x_{122} & x_{132} & x_{212} & x_{222} & x_{232} \\ x_{113} & x_{123} & x_{133} & x_{213} & x_{223} & x_{233} \end{bmatrix}.$$

The $(t+1)$-minors of the various unfolding matrices are contained in the ideal defining the t-secant variety of the Segre variety but, in general, one needs extra generators. We prove that for the tensor of size $(2,a,b)$ the $(t+1)$-minors coming from the unfolding matrices are enough to generate $I(a,b)^{\{t\}}$. More precisely:

Theorem Let K be a field of arbitrary characteristic and a, b positive integers. Then

(1) the defining ideal $I(a,b)^{\{t\}}$ of the t-secant variety $\sigma_t(2,a,b)$ of the Segre variety $\mathrm{Seg}(2,a,b)$ is $I_{t+1}(\mathcal{X}^{\{2\}}) + I_{t+1}(\mathcal{X}^{\{3\}})$.

(2) the $(t+1)$-minors of $\mathcal{X}^{\{2\}}$ and $\mathcal{X}^{\{3\}}$ are a Gröbner basis of $I(a,b)^{\{t\}}$ with respect to any diagonal term order.

(3) $R/I(a,b)^{\{t\}}$ is a Cohen-Macaulay domain.

These results are already known in characteristic 0, see [4], while our results are valid in arbitrary characteristic. Furthermore our construction allows us to give a formula for the degree of the secant varieties $\sigma_t(2,a,b)$, and to give a bound for their Castelnuovo-Mumford regularity; this bound is sharp if $2t \leq b$.

Theorem The ring $R/I(a,b)^{\{t\}}$ is a domain of dimension $(a+b)t$, and of multiplicity

$$\sum_{1 \leq h_1 < \cdots < h_t \leq b} \det(g_{ij})$$

with $g_{ij} = \binom{a+b-h_j+h_i-1}{a-1}$ for $1 \leq i,j \leq t$. Furthermore the Castelnuovo Mumford regularity of $R/I(a,b)^{\{t\}}$ is $\leq at$, with equality if $b \geq 2t$.

We also state this conjecture, which we prove to be true for $t \leq 3$:

Conjecture For any t the ring $R/I(2t,2t)^{\{t\}}$ is Gorenstein.

Related interesting results have been obtained indipendently by Fieldsteel and Klein in [2].

Keywords
Tensor, Determinantal rings, Segre product

References

[1] A. Conca, E. De Negri, Z. Stojanac, Determinantal ideals of 3-tensors, *Algebraic Combinatorics* **3** (no. 5), 1011–1021 (2020).

[2] N. Fieldsteel, P. Klein , Gröbner bases and the Cohen-Macaulay property of Li's double determinantal varieties. *Proc. Amer. Math. Soc. Ser. B* **7**, 142–158 (2020).

[3] T. Hibi, Distributive lattices, affine semigroup rings and algebras with straightening laws, Commutative Algebra and Combinatorics. In *Adv. Stud. Pure Math.*, M. Nagata, H. Matsumura (eds), 93–109, Mathematical Society of Japan, Kyoto, 1987.

[4] J.M. LANDSBERG; J. WEYMAN, On the ideals and singularities of secant varieties of Segre varieties. *Bull. Lond. Math. Soc.* **39**(4), 685-697 (2007).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Algebraic geometry from an algorithmic point of view "*

A practical method to compute the geometric Picard lattice of K3 surfaces of degree 2

Dino Festi[1] [dino.festi@unimi.it]

[1] Dipartimento di Matematica "Federigo Enriques", Università degli Studi di Milano, Milano, Italy

A smooth surface X over a field k is defined to be a K3 surface if and only if its first cohomology group $H^1(X, \mathcal{O}_X) = 0$ is trivial as well as its canonical divisor $K_X \sim_{\text{lin}} 0$. Smooth quartic surfaces in $\mathbb{P}^3$ and double covers of $\mathbb{P}^2$ ramified above a smooth sextic curve are examples of K3 surfaces.

If X is a K3 surface over a field k, and $\operatorname{Div} X$ denotes its divisor group, we define the *Picard group* of X to be the quotient $\operatorname{Div} X/\sim_{\text{lin}}$. Let $\overline{k}$ be an algebraic closure of k; we define $\overline{X} := X \times_k \overline{k}$ to be the base change of X to $\overline{k}$. We define the *geometric Picard group* of X to be $\operatorname{Pic} \overline{X}$. The intersection pairing on $\operatorname{Div} X$ induces a pairing on $\operatorname{Pic} X$, also called intersection pairing; $\operatorname{Pic} X$ endowed with the intersection pairing turns out to be an even lattice. Computing the geometric Picard lattice of a K3 surface X basically means computing a Gram matrix of the lattice $\operatorname{Pic} \overline{X}$.

K3 surfaces are often described as surfaces of intermediate type, i.e., they are in between the surfaces whose geometry and arithmetic is well understood (rational and ruled surfaces) and those surfaces whose geometry and arithmetic is still largely unknown (surfaces of general type). From that point of view, K3 surfaces are the two-dimensional analogues of elliptic curves. For this reason, K3 surfaces are extremely interesting objects to study and an important testing ground for conjectures regarding surfaces. In addition, K3 surfaces often appear in contexts other than geometry: problems in number theory and physics have often led to the study of the geometry and/or the arithmetic of particular K3 surfaces.

In the study of a K3 surface, its geometric Picard lattice plays a crucial role. Knowing it, it is possible to derive much information about the geometry and the arithmetic of the surface, for example: the potential density of rational points of a K3 surface defined over a number field; the algebraic part of the Brauer group; the existence of elliptic fibrations; whether X is isomorphic to a Kummer surface or not. This is why the growing interest in K3 surfaces in the last years induced a growing interest in the computation of the Picard lattice of a K3 surface.

Despite its importance and the attention given to it, computing the Picard lattice stays, in general, a hard problem. Assuming the Tate conjecture and the computability of étale cohomology with finite coefficients, Poonen, Testa and van Luijk give an algorithm to compute the Picard lattice of any smooth projective geometrically integral variety, and hence also for any K3 surface (cf. [9]). In [6], Hassett, Kresch, and Tschinkel give an effective algorithm to compute the Picard lattice of K3 surfaces of degree two over a number field. A practical, numerical method to compute the Picard lattice of a K3 surface given by a smooth quartic in $\mathbb{P}^3$ is given by P. Lairez and E. Can Sertöz in [7].

The method by Poonen, Testa and van Luijk to compute the Picard lattice of any K3 surface and the one by Hassett, Kresch and Tschinkel are far from being practical and have, to the best of our knowledge, never been used in practice, let alone implemented in any computer algebra. On the contrary, the algorithm proposed by Lairez and Can Sertöz is very practical, and it has been successfully tested on a large number of surfaces. Although very precise in practice, this method does not return proven correct answers, as a certification of the numerical computations involved is still lacking (see [7, §§1, 4-5]). This situation leaves the computation of the (geometric) Picard lattice of a K3 surface a problem still open.

In this talk I am going to present a practical method to compute the geometric Picard lattice of a K3 surface of degree 2 over number fields and finitely generated function fields over number fields (cf. [4]). In general, the main challenge in computing the Picard lattice of a K3 surface X is to find enough divisors. K3 surfaces of degree 2 come with a natural structure of double covers of $\mathbb{P}^2$ branched above a sextic curve $B \subset \mathbb{P}^2$. The basic idea of the method presented here is to exploit this structure to find divisors. In particular, rational plane curves that are everywhere tangent to branch locus B provide divisors of X that are not linearly equivalent to a hyperplane section. So the problem of finding divisors on X is translated to find plane genus 0 curves that intersect B everywhere with even multiplicity. We remark that all the divisors obtained in this way are -2 curves on X (in the sense the intersection pairing evaluated on the curve and itself is -2). Once these divisors are obtained, we compute the sublattice $\Lambda \subseteq \operatorname{Pic} \overline{X}$ they generate. This part can be easily dealt by a computer. The final step is to check whether $\Lambda = \operatorname{Pic} \overline{X}$ or not. This check heavily relies on the ability of finding a sharp upper bound r for the rank of $\operatorname{Pic} \overline{X}$ and can only be applied if $\operatorname{rk} \Lambda = r$. If this is the case, then for every prime p such that p^2 divides the discriminant of Λ, we compute the set

$$\Lambda_p := \left\{ [x] \in \Lambda/p\Lambda \mid \forall\, [y] \in \Lambda/p\Lambda \ \ [x].[y] = 0 \text{ and } x^2 \equiv 0 \bmod 2p^2 \right\}.$$

If all these Λ_p are equal to $\{0\}$, then Λ is the full geometric Picard lattice and we are done. If some of these sets are not trivial, one can still use the automorphism group of X or the Galois action on $\operatorname{Pic} \overline{X}$ to try to conclude that $\Lambda = \operatorname{Pic} \overline{X}$ (cf. [4, Proposition 7.7]).

The method is practical in the sense that it can and has been successfully used in practice (see [1, 3, 5]); under certain circumstances it might not terminate, but if it terminates it returns a proven correct answer. In particular, there are three cases which might lead the algorithm to not terminate: the upper bound r for the rank of the Picard lattice is not sharp; the Picard lattice cannot be generated by the hyperplane section and -2-curves; the subsets Λ_p are too big. Notice that in the first and third cases, the method might still provide the full geometric Picard lattice and 'only' fail to prove it. Unfortunately, we are not aware of any practical way to assess whether any of these three is going to occur for a given K3 surface. For a more detailed analysis of the issues that might prevent the method from terminating we refer to [4, §8]. The method is also suitable for K3 surfaces with ADE singularities.

As an example, one can look at the 1-dimensional family $\mathcal{X}$ of K3 surfaces considered in [3] and compute the geometric Picard lattice of the generic member X. One can use van Luijk's method (cf. [10]) to show that $\operatorname{rk}\operatorname{Pic}\overline{X} \leq 19$. Then, by looking at conics everywhere tangent to the branch locus, one can find many divisors (more than 400). These divisors generate a sublattice $\Lambda \subseteq \operatorname{Pic}\overline{X}$ of rank 19. Then one proceeds as above to show that $\Lambda = \operatorname{Pic}\overline{X}$.

This algorithm has been partially implemented in `Magma` [2] in the package about degree two K3 surfaces, see [8]. A full independent implementation of this method together with an optimization for K3 surfaces admitting elliptic fibrations are currently work in progress.

Keywords
K3 surfaces, Picard lattice.

References

[1] M. Besier; D. Festi; M. Harrison; B. Naskręcki, Arithmetic and geometry of a K3 surface emerging from virtual corrections to Drell-Yan scattering. *Commun. Number Theory Phys.* **14**(4), first 863–911 (2020).

[2] W. Bosma; J. Cannon; C. Playoust, The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24**(3-4), 235–265 (1997).

[3] F. Bouyer; E. Costa; D. Festi; C. Nicholls; M. West, On the arithmetic of a family of degree-two K3 surfaces. *Math. Proc. Cambridge Philos. Soc.* **166**(3), 523–542 (2019).

[4] D. Festi, A practical algorithm to compute the geometric Picard lattice of K3 surface of degree 2. `arXiv:1808.00351` (2018).

[5] D. Festi; D. van Straten, Bhabha scattering and a special pencil of K3 surfaces. *Commun. Number Theory Phys.* **13**(2), 463—485 (2019).

[6] B. Hassett; A. Kresch; Y. Tschinkel, Effective computation of Picard groups and Brauer-Manin obstructions of degree two $K3$ surfaces over number fields. *Rend. Circ. Mat. Palermo (2)* **62**(1), 137—151 (2013).

[7] P. Lairez; E. Can Sertöz, A numerical transcendental method in algebraic geometry: computation of Picard groups and related invariants. *SIAM J. Appl. Algebra Geom.* **3**(4), first 559—584 (2019).

[8] Magma, Package on Degree 2 K3 surfaces, `http://magma.maths.usyd.edu.au/magma/handbook/text/1434`.

[9] B. Poonen; D. Testa; R. van Luijk, Computing Néron-Severi groups and cycle class groups. *Compos. Math.* **151**(4), 713—734 (2015).

[10] R. van Luijk, K3 surfaces with Picard number one and infinitely many rational points. *Algebra Number Theory*, **1**(1), 1—15 (2007).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Algebraic Geometry from an Algorithmic Point of View"*

Gluing semigroup rings and the Cohen-Macaulay property

Philippe Gimenez[1][*], ***Hema Srinivasan***[2] [pgimenez@uva.es]

[1] Mathematics Research Institute (IMUVA), Univ. of Valladolid, Spain
[2]Department of Mathematics, Univ. of Missouri, Columbia, USA

Consider the semigroup $\langle A\rangle$ finitely generated by a subset $A=\{\mathbf{a}_1,\ldots,\mathbf{a}_p\}$ of $\mathbb{N}^n$, let k be an arbitrary field and $\phi_A : k[x_1,\ldots,x_p]\to k[t_1,\ldots,t_n]$ be the ring homomorphism defined by $\phi_A(x_j)=t^{\mathbf{a}_j}=\prod_{i=1}^n t_i^{a_{ij}}$ where $\mathbf{a}_j=\begin{pmatrix}a_{1j}\\ \vdots\\ a_{nj}\end{pmatrix}\in\mathbb{N}^n$. The kernel of ϕ_A, $I_A=\ker(\phi_A)$, is a binomial prime ideal and the semigroup ring $k[A]$ is isomorphic to $k[x_1,\ldots,x_p]/I_A$. We will also denote by A the $n\times p$ integer matrix whose columns are the elements in A. It is well-known that the Krull dimension of the semigroup ring $k[A]$ coincides with the rank of the matrix A.

For a semigroup $\langle C\rangle$, when the set of generators of the semigroup splits into two disjoint parts, $C=A\cup B$, such that by $I_C=I_A+I_B+\langle\rho\rangle$ where ρ is a binomial whose first, respectively second, monomial involves only variables corresponding to elements in A, respectively B, we say that $\langle C\rangle$ is a *gluing* of $\langle A\rangle$ and $\langle B\rangle$. This property can be characterized in terms of the semigroups $\langle A\rangle$ and $\langle B\rangle$ and the subgroups in $\mathbb{Z}^n$ associated to them; see [6, Thm. 1.4].

Gluing has its origin in the study of the structure of affine semigroup rings that are complete intersections. Inspired by the classical construction by Delorme in [2] for the study and characterization of complete intersection numerical semigroups, Rosales introduced in [6] the concept of gluing. The structure of affine semigroup rings that are complete intersections is completely described in [7] for simplicial semigroups and later generalized in [3]: a semigroup is a complete intersection if and only if it is a gluing of two complete intersections of smaller embedding dimension. But the gluing operation is interesting by itself for semigroups that are not complete intersections.

Let's first fix some notations. If we have two semigroups $\langle A\rangle$ and $\langle B\rangle$ in $\mathbb{N}^n$ with $A=\{\mathbf{a}_1,\ldots,\mathbf{a}_p\}$ and $B=\{\mathbf{b}_1,\ldots,\mathbf{b}_q\}$, variables corresponding to A, respectively B, will

[*]The first author was partially supported by *Ministerio de Ciencia e Innovación* (Spain) PID2019-104844GB-I00.

be denoted by $x_1, \ldots, x_p$, respectively $y_1, \ldots, y_q$. Thus, $I_A \subset k[x_1, \ldots, x_p]$, $k[A] \simeq k[x_1, \ldots, x_p]/I_A$, $I_B \subset k[y_1, \ldots, y_q]$ and $k[B] \simeq k[y_1, \ldots, y_q]/I_B$. If the generating set C of a semigroup $\langle C \rangle$ splits into two disjoint parts $C = A \cup B$, then $I_C \subset R = k[x_1, \ldots, x_p, y_1, \ldots, y_q]$ and $k[C] \simeq R/I_C$. Since multiplying by a common integer all the elements in the generating set of a semigroup does not change the defining ideal of the semigroup ring, one can easily check that if $C = k_1 A \cup k_2 B$ for some nonnegative integers k_1 and k_2, then $I_C \cap k[x_1, \ldots, x_p] = I_A (= I_{k_1 A})$ and $I_C \cap k[y_1, \ldots, y_q] = I_B (= I_{k_2 B})$. Note that if one gives weight $k_1 \mathbf{a}_i$ to x_i and $k_2 \mathbf{b}_j$ to y_j for all i, j, then the ring $k[C]$ is graded over the semigroup $\langle C \rangle$.

In [4], the structure of the minimal free resolution of semigroup rings obtained by gluing is given in terms of the minimal free resolutions of the two semigroup rings glued: if $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_p\}$ and $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_q\}$ are two finite subsets of $\mathbb{N}^n$ and $\langle C \rangle$ is a gluing of $\langle A \rangle$ and $\langle B \rangle$, i.e., $C = A \cup B$ and $I_C = I_A + I_B + \langle \rho \rangle$ for some $\rho = \underline{\mathrm{x}}^{\alpha} - \underline{\mathrm{y}}^{\beta}$ with $\alpha \in \mathbb{N}^p$ and $\beta \in \mathbb{N}^q$, given F_A and F_B minimal graded free resolutions of $k[A]$ and $k[B]$, one has by [4, Thm. 6.1 & Cor. 6.2] that:

1. A minimal graded free resolution of $k[C]$ can be obtained as the mapping cone of $\rho : F_A \otimes F_B \to F_A \otimes F_B$ where ρ is induced by multiplication by ρ.
2. The Betti numbers of $k[A]$, $k[B]$ and $k[C]$ are related as follows: $\forall i \geq 0$,

$$\begin{aligned} \beta_i(k[C]) &= \sum_{i'=0}^{i} \beta_{i'}(k[A])[\beta_{i-i'}(k[B]) + \beta_{i-i'-1}(k[B])] \\ &= \sum_{i'=0}^{i} \beta_{i'}(k[B])[\beta_{i-i'}(k[A]) + \beta_{i-i'-1}(k[A])] \,. \end{aligned}$$

3. In particular, the relation between the projective dimensions of $k[A]$, $k[B]$ and $k[C]$ is:

$$\mathrm{pd}(k[C]) = \mathrm{pd}(k[A]) + \mathrm{pd}(k[B]) + 1 \,.$$

In [5], we go one step forward and try to understand when two semigroups can be glued and, when it is possible, how to glue them. We also give some partial information on how gluing works in the Cohen-Macaulay case (that includes complete intersections, the origin of the problem). In this talk, we will generalize the results in [5] and completely characterize the Cohen-Macaulay property showing that if $\langle A \rangle$ and $\langle B \rangle$ can be glued and $\langle C \rangle$ is a gluing of $\langle A \rangle$ and $\langle B \rangle$, then:

1. $k[C]$ is Cohen-Macaulay if and only if $k[A]$ and $k[B]$ are.
2. $k[C]$ is Gorenstein if and only if $k[A]$ and $k[B]$ are.
3. $k[C]$ is a complete intersection if and only if $k[A]$ and $k[B]$ are.

We will classify all possible gluing in small dimension and provide non-trivial examples. The above results allow to build Cohen-Macaulay or Gorenstein semigroups of arbitrary high

dimension and embedding dimension if one knows how to glue two semigroups. We will see that degeneracy is necessary in order to glue two semigroups except in the case of numerical semigroups that can always be glued. All computations are done using Singular [1].

Keywords

semigroup rings, gluing, syzygy, Betti numbers, Cohen-Macaulay, Gorenstein

References

[1] W. DECKER; G.-M. GREUEL; G. PFISTER; H. SCHÖNEMANN, Singular 4-2-0, a computer algebra system for polynomial computations. http://www.singular.uni-kl.de (2020).

[2] C. DELORME, Sous-monoïdes d'intersection complète de $\mathbb{N}$. *Ann. Sci. École Norm. Sup. (4)* **9**, 145-154 (1976).

[3] K. G. FISCHER; W. MORRIS; J. SHAPIRO, Affine semigroup rings that are complete intersections. *Proc. Amer. Math. Soc.* **125**, 3137-3145 (1997).

[4] P. GIMENEZ; H. SRINIVASAN, The structure of the minimal free resolution of semigroup rings obtained by gluing. *J. Pure Appl. Alg.* **223**, 1411-1426 (2019).

[5] P. GIMENEZ; H. SRINIVASAN, Gluing semigroups: when and how. *Semigroup Forum* **101**, 603-618 (2020).

[6] J. C. ROSALES, On presentations of subsemigroups of $\mathbb{N}^n$. *Semigroup Forum* **55**, 152-159 (1997).

[7] J. C. ROSALES; P. A. GARCÍA-SÁNCHEZ, On complete intersection affine semigroups. *Comm. Algebra* **23**, 5395-5412 (1995).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Algebraic Geometry from an algorithmic point of view"*

The Gröbner fan of the Hilbert scheme

Paolo Lella[1] [paolo.lella@polimi.it]

[1] Dipartimento di Matematica, Politecnico di Milano, Milan, Italy

The Hilbert scheme $\mathbf{Hilb}^n_{p(t)}$, parametrizing subschemes of $\mathbb{P}^n$ with Hilbert polynomial $p(t)$, has been intensively studied since its definition and proof of existence by Grothendieck. Nevertheless, very few comprehensive properties are known and lots of natural questions are still open. The problem of understanding the topological structure of the Hilbert scheme is usually complicated due to its unpredictable and mysterious behavior. Questions such "how many irreducible components are there in $\mathbf{Hilb}^n_{p(t)}$?", "how are the irreducible components related?", "are the irreducible components rational?" are in most cases without a complete answer.

In this context, a classical approach consists in trying to rephrase a global question in terms of a local question for a few, possibly finite, number of points of $\mathbf{Hilb}^n_{p(t)}$. An efficient way to accomplish this task is to consider Gröbner degenerations to monomial ideals and in particular to generic initial ideals. Indeed, on one hand each irreducible component and each intersection of irreducible components of $\mathbf{Hilb}^n_{p(t)}$ contains at least one point corresponding to a generic initial ideal. On the other hand, generic initial ideals are Borel-fixed ideal, i.e. invariant under the action of the Borel subgroup of $\mathrm{GL}_{\mathbb{K}}(n+1)$ consisting of upper triangular matrices. Furthermore, in characteristic 0, Borel-fixed ideals enjoy additional combinatorial properties. Hence, Borel-fixed ideals are well distributed throughout the Hilbert scheme and have special properties that make them extremely effective.

The content of this work is strongly influenced by the theory of Gröbner strata and marked families (see [3] and references therein). Given a Borel-fixed ideal J and a term order Ω, the Gröbner stratum $\mathbf{St}^{\Omega}_J$ is the scheme parametrizing the family of ideals with initial ideal J with respect to Ω. The marked scheme $\mathbf{Mf}_J$ is the scheme parametrizing the family of ideals whose quotient algebras have the set of monomials not contained in J as basis. These families can be used to parametrize open subsets of $\mathbf{Hilb}^n_{p(t)}$ (or of one of its irreducible component) or sub-loci corresponding to schemes with special properties (such as Hilbert function, type of resolution, . . .).

However, if one is interested in studying the irreducible components of $\mathbf{Hilb}^n_{p(t)}$, the set of Borel-fixed ideals turns out to be redundant, in a sense clarified by the following example.

Example. Consider the Hilbert scheme $\mathbf{Hilb}^3_{6t-3}$ parametrizing 1-dimensional subschemes of $\mathbb{P}^3$ of degree 6 and arithmetic genus 4. There are 3 irreducible components:

- the first component has dimension 48 and the general element is the union of a plane curve of degree 6 and 6 isolated points;
- the second component has dimension 32 and the general element is the union of a plane quintic and a line intersecting in one point, and 2 isolated points;
- the third component has dimension 24 and the general element is a complete intersection of a quadric surface and a cubic surface.

By the theory of marked families, in order to parametrize an open subset of each irreducible component, we need at most 3 Borel-fixed ideals. In $\mathbf{Hilb}^3_{6t-3}$ there are 31 points corresponding to Borel-fixed ideals to choose from, whose algebraic and geometric properties are very diverse. First, such points are not equally distributed along the irreducible components. In fact, most of them lie exclusively on the first irreducible component. Second, there are smooth points, singular points lying on a single component and singular points that are in the intersection of 2 irreducible components and that are smooth if we restrict to any of them. Third, these points have different behavior with respect to Gröbner degenerations.

Two natural questions arise.

(Q1) Assume that the topological structure of the Hilbert scheme and the distribution between components of points corresponding to Borel-fixed ideals are known. Which ones are better suited for effective investigation?

(Q2) Suppose that one knows nothing about the Hilbert scheme, but the list of Borel-fixed ideals defining points on it. Is it possible to deduce information about the topological structure of $\mathbf{Hilb}^n_{p(t)}$?

These two problems are discussed in the inspiring paper "Double-generic initial ideal and Hilbert scheme" [1]. The double-generic initial ideal is a Borel-fixed ideal associated to an irreducible component of $\mathbf{Hilb}^n_{p(t)}$. Intuitively, it is the generic initial ideal of the ideal describing the generic element of the component. Hence, choosing the double-generic initial ideal among Borel-fixed ideals lying on a given component is a reasonable and natural option to answer *(Q1)*. Still, there are some difficulties. First of all, the double-generic initial ideal is not intrinsically determined by an irreducible component, but it depends on the term order. Secondly, if we do not know a priori the list of Borel-fixed ideals defining points on a given irreducible component, we might not be able to detect the corresponding double-generic initial ideal with respect to a fixed term order (this makes it difficult to answer *(Q2)*).

The definition of the double-generic initial ideal is based on a careful analysis of the action of the linear group on the generators of an ideal defining a point on the Hilbert scheme. In this work, we use a different approach based on the study of the combinatorial properties of Borel-fixed ideals. In particular, the combinatorics allow to better understand the behavior of the points of the Hilbert scheme under Gröbner degenerations (and thus also the dependence of double-generic initial ideal on the term order).

A first result is about the relative position of points corresponding to Borel-fixed ideals in the Hilbert scheme.

Theorem [2, Definition 3.1 and Theorem 3.5]**.** *Let $J, J' \subset \mathbb{K}[x_0,\ldots,x_n]$ be two saturated Borel-fixed ideals defining points on $\mathbf{Hilb}^n_{p(t)}$ and denote by $\mathfrak{J}$ and $\mathfrak{J}'$ the monomial bases of*

J_r and J'_r for r sufficiently large. If the monomials in the sets $\mathfrak{J} \setminus \mathfrak{J}'$ and $\mathfrak{J}' \setminus \mathfrak{J}$ have the same linear syzygies, then there is a rational curve on $\mathbf{Hilb}^n_{p(t)}$ passing through the points defined by J and J'.

As a consequence of this result, we introduce the Borel graph of $\mathbf{Hilb}^n_{p(t)}$ whose vertices correspond to Borel-fixed ideals and whose edges correspond to unordered pairs of ideals satisfying the hypothesis of the previous theorem. Any term order induces an orientation of the edges of the Borel graph producing a directed graph. Then, we classify all these directed graphs, by means of a polyhedral fan that we call *Gröbner fan of the Hilbert scheme*. Each cone of maximal dimension corresponds to a different directed graph where the orientation of the edges is induced by some term order.

For several degeneration graphs, we are able to construct a minimum spanning tree. This implies that the Borel graph is a connected graph and gives a new strategy to prove the connectedness of the Hilbert scheme.

Theorem [2, Theorem 5.8]**.** *The Hilbert scheme is rationally chain connected.*

In the degeneration graphs having a minimum spanning tree, there is a unique vertex with no incoming edge. Typically, this is not the case. Rather the number of vertices with no incoming edge in a degeneration graph can give interesting information about the topological structure of the Hilbert scheme (answering *(Q2)*). Exploiting again properties of double-generic initial ideals, we can give the following lower bound on the number of irreducible components of the Hilbert scheme.

Theorem [2, Proposition 5.14 and Conjecture 5.17]**.** *The number of irreducible components of $\mathbf{Hilb}^n_{p(t)}$ is at least the maximum number of vertices with no incoming edge in any degeneration graph.*

In order to obtain the best estimate, one has to examine a finite number of degeneration graphs, one for each cone of maximal dimension of the Gröbner fan. For instance, in the case of the Hilbert scheme $\mathbf{Hilb}^3_{6t-3}$, the Gröbner fan has 268 cones of maximal dimension and the maximum number of vertices with no incoming edge in a degeneration graph is 3. Hence, in this case our method detects all the irreducible components of the Hilbert scheme and it also suggests three Borel-fixed ideals to consider to parametrize the components via marked families.

Keywords
Hilbert scheme, strongly stable ideal, Gröbner degeneration, polyhedral fan, connectedness, irreducibility

References

[1] C. Bertone; F. Cioffi; M. Roggero, Double-generic initial ideal and Hilbert scheme, *Ann. Mat. Pura Appl. (4)* **196**(1), 19–41 (2017).

[2] P. Lella; Y. Kambe, The Gröbner fan of the Hilbert scheme, *Ann. Mat. Pura Appl. (4)* **200**(2), 547–594 (2021).

[3] P. Lella; M. Roggero, On the functoriality of marked families, *J. Commut. Algebra* **8**(3), 367–410, (2016).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic Geometry from an Algorithmic Point of View”*

Why you should never think of using Gröbner bases in Algebraic Statistics

Michela Ceria[1], ***Theo Moriarty***[2] [5919@unige.it]

[1] Dipartimento di Meccanica, Matematica e Management, Politecnico di Bari, Via Orabona 4, I-70125 Bari, Italy
[2] SPECTRE, Cayman Islands

In [5] Lauenbacher and Stigler applied Groebnerian technologies to data modelling, their input being a set $\mathbf{X} = \{P_1, \dots, P_N\} \subset (\mathbb{Z}_p)^n$ of N points P_i, $1 \le i \le N$ with coordinates in $\mathbb{Z}_p, p$ a prime, and their output the normal forms modulo the ideal of points $I(\mathbf{X})$ of the polynomials

$$f_j : (\mathbb{Z}_p)^n \to \mathbb{Z}_p, 1 \le j \le n : (f_1(P_i), \dots, f_n(P_i)) = P_{i+1}, i = 1, \dots, N-1. \tag{1}$$

They applied Lagrange Intepolation, Chinese Remainder Theorem, Buchberger-Möller Algorithm [2,8,11] in order to obtain the Gröbner basis of $I(\mathbf{X})$ and Buchberger reduction to obtain the required normal form. Their (correct) evaluation of the complexity[*] of their algorithm was

$$O(n^2N^2) + O((N^3 + N)f + N^2n^2) + O(n(N-1)2^{cN+N-1}).$$

In [4] we gave a better analysis of their algorithm granting it the classical FGLM-complexity $O(N^2nlog(N)) + O(n^2N^3f)$ but we applied the degrobnerization tecniques proposed by Lundqvist [7] and Ceria [3] granting the “degrobnerization complexity”[†] $O(nN^2 \log(N)) + O(nN^{O(1)}f)$.

The main difference between [5] and [4] consists in alternative and opposite approaches to describe and process their data:

- Lauenbacher and Stigler [5] (but also [18] and [19]) preserve all their data as *polynomials* $f \in \mathbf{k}[x_1, \dots, x_n]$; consequently, they describe the ideal $I(\mathbf{X})$ in the framework

[*] where the value f introduced in [8] measures the “distributed cost” of evaluating s functionals at a normal set of cardinality c which is evaluated fcs; the value f, which is $(\log(p))^2$ for the case $\mathbf{k} = \mathbb{Z}_p$, in the more important case $\mathbf{k} = \mathbb{Q}$ has been evaluated in [2, Th.4.1, Th.4,2] by proposing a *modular BM-algorithm* based on Chinese Remaindering techniques as $f := N^3(\log(p))^2$ for each termordering and $f := N^2d(\log(p))^2$ for the important case of “generic” points and the degrevlex ordering where g is the number of the elements of the required Gröbner basis and d is such that $\binom{n+d-1}{d} = N + g$.

[†] The point is that the approach is no more quadratic, but just linear, on the number of variables.

of Buchberger theory, giving its Gröbner basis $\mathcal{G}$ and they produce their output via Buchberger reduction.

- Degroebnerization describes the same ideal in Lundqvist's framework [7] via a *normal set*
$$\mathsf{N} = \{t_1, \ldots, t_N\} \subset \mathbf{k}[x_1, \ldots, x_n]$$
such that $[\mathsf{N}] = \{[t_1], \ldots, [t_N]\}$ is a *linear basis* for $A := \mathbf{k}[x_1, ..., x_n]/I = \mathrm{Span}_{\mathbf{k}}[\mathsf{N}]$ and produces its output by evaluation of the monomials in N at the points $\mathbf{X}$ using Theorem 1 [7] below.

Theorem 1. *Let $\mathbf{X} = \{P_1, ..., P_N\}$ be a finite set of simple points, $I := I(\mathbf{X}) \lhd \mathbf{k}[x_1, ..., x_n]$ the ideal of points and $\mathsf{N} = \{t_1, ..., t_N\} \subset \mathbf{k}[x_1, ..., x_n]$ such that $[\mathsf{N}] = \{[t_1], ..., [t_N]\}$ is a basis for $A := \mathbf{k}[x_1, ..., x_n]/I$. Then, for each $f \in \mathbf{k}[x_1, ..., x_n]$ we have*

$$\mathrm{Nf}(f, \mathsf{N}) = (t_1, ..., t_N)(\mathsf{N}[\mathbf{X}]^{-1})^t(f(P_1), ..., f(P_N))^t,$$

where $\mathsf{N}[\mathbf{X}]$ is the matrix whose rows are the evaluations of N at the elements of $\mathbf{X}$ and Nf(f, N) is the normal form of f w.r.t. $I(\mathbf{X})$.

Degroebnerization is a new approach in Computer Algebra proposed by many papers [7,10,15,16,21] which has been explicitly expressed and endorsed in [9 Vol.3, 40.12,41.15]; it means avoiding Gröbner basis computation and Buchberger's reduction as much as possible, leaving their use to the only cases in which it is really necessary, mainly using linear algebra and combinatorial methods.

Consequently

- in [5] the authors preliminarly translate their data in the chosen framework, namely they pass from points to polynomials and they perform all their computations with polynomials, directly obtaining the desired ouput

while

- degroebnerization preliminarly performs all its computations using combinatorics on the points and on the monomials of the quotient algebra basis and only in the end translates its data into polynomials, returning the desired ouput, using Theorem 1.

In a further paper [6] Lauenbacher and Stigler apply their tool to *design of experiments* remarking that their algorithm described in [5] can be applied simply adapting Eq.(1) after redefining F as

$$F(P_i) = (f_1(P_i), \ldots, f_n(P_i)) = Q_i, i = 1, \ldots, N;$$

thus, in principle, the same arguments, algorithms, analysis developped in [4] can be *verbatim* extended to this algebraic statistic problem.

The main advocate of a Groebnerian approach, via the Buchberger-Möller Algorithms improved, extended and generalized in [2], is [19] which however points to some difficulties in such applications; for instance the interest to *linear models whose vector space basis is formed by polynomials v_j which are not monomials* [19, pg.102] and the potential interest, for their symmetric features [19, pg.114], of *Hierarchical Monomial Bases* which are not *corner cuts* [17], not being a normal set w.r.t. a Gröbner basis [19, Ex.7]].

The main tool for their Gröbnerian applications, according [18] and [6], apparently is [20, Th.4.12], which however is stated and holds not only for a normal set, but in a more general setting, thus including all the constructions based as the one of [2] on the notion of *border basis* introduced in [8]; this includes in particular Mourrain's [15, Def.2.6] concept of *connected to 1* and Mora's, deeply depending on Mourrain's [15,16] results, *le degree zero de Möller* which probably will never be published but which has been presented for the first time in 2010 at a course at Trento's CryptoLabTN [12], implicitly in a commutative setting, but later explicitly in a non-commutative settings at ACA2018 [13] and UMI2019 [14]; *le degree zero de Möller* allows to describe a (finite) vector space V as a $\mathbf{k}$-module over a (not-necessarily commutative) polynomial ring over a finite set of variables $x_1, \dots, x_n$ by giving a linear basis $\{v_1, \dots, v_N\}$ of it and describing the action of variables by classical Auzinger-Stetter [1] matrices; under this description a design can therefore be described as a *design ideal* $\mathcal{I} \subset \mathcal{P} : V = \mathcal{P}/\mathcal{I}$, with either $\mathcal{P} = \mathbf{k}[x_1, \dots, x_n]$ or $\mathcal{P} = \mathbf{k}\langle x_1, \dots, x_n\rangle$; with this representation [20, Th.4.12] holds, design of experiments can be described as ideals of $V = \mathcal{P}/\mathcal{I}$ and normal forms can be obtained via Lundqvist's approach.

Example 2. We describe the design ideal with $I(\mathcal{F})$,

$$\mathcal{F} := \{(0,0), (1,-1), (-1,1), (0,1), (1,0)\},$$

the Hierarchical Monomial Bases (but not a corner cut) $\{1, x, x^2, y, y^2\}$ discussed in [Ex.7][19]

Degrobnerization produces the suitable basis $\mathsf{N} := \{1, x, \frac{x^2-x}{2}, y+x, -y^2+x^2+y+x\}$ of $\mathbf{k}[x_1, \dots, x_n]/I(\mathcal{F})$, the matrix

$$\mathsf{N}[\mathcal{F}] = \left|\begin{array}{r|ccccc} & (0,0) & (1,-1) & (-1,1) & (0,1) & (1,0) \\ \hline 1 & \mathbf{1} & 1 & 1 & 1 & 1 \\ x & 0 & \mathbf{1} & -1 & 0 & 1 \\ \frac{x^2-x}{2} & 0 & 0 & \mathbf{1} & 0 & 0 \\ y+x & 0 & 0 & 0 & \mathbf{1} & 1 \\ \frac{-y^2+x^2+y+x}{2} & 0 & 0 & 0 & 0 & \mathbf{1} \end{array}\right|$$

and the Auzinger-Stetter [1] matrices

$$A_x = \left.\begin{array}{r|ccccc} & 1 & x & x^2 & y & y^2 \\ \hline 1 & 0 & 1 & 0 & 0 & 0 \\ x & 0 & 0 & 1 & 0 & 0 \\ y & 0 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ x^2 & 0 & 1 & 0 & 0 & 0 \\ y^2 & 0 & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{array}\right|, \quad A_y = \left.\begin{array}{r|ccccc} & 1 & x & x^2 & y & y^2 \\ \hline 1 & 0 & 0 & 0 & 1 & 0 \\ x & 0 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ y & 0 & 0 & 0 & 0 & 1 \\ x^2 & 0 & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ y^2 & 0 & 0 & 0 & 1 & 0 \end{array}\right|.$$

Lundqvist's result applies Gaussian reduction in order to transform the triangular set $V = \{v_i, 1 \leq i \leq 5\}$ into the separating set obtaining at the same time the matrix $\left(I|A^{-1}\right)$ and the separating set

$$W = \{w_i, 1 \leq i \leq 5\} = A^{-1}V;$$

thus from

		$(0,0)$	$(1,-1)$	$(-1,1)$	$(0,1)$	$(1,0)$					
v_1	1	$\mathbf{1}$	1	1	1	1	1	0	0	0	0
v_2	x	0	$\mathbf{1}$	-1	0	1	0	1	0	0	0
v_3	$\frac{x^2-x}{2}$	0	0	$\mathbf{1}$	0	0	0	0	1	0	0
v_4	$y+x$	0	0	0	$\mathbf{1}$	1	0	0	0	1	0
v_5	$\frac{-y^2+x^2+y+x}{2}$	0	0	0	0	$\mathbf{1}$	0	0	0	0	1

we obtain

		$(0,0)$	$(1,-1)$	$(-1,1)$	$(0,1)$	$(1,0)$					
w_1	$1-\frac{y^2+x^2+y+x}{2}$	$\mathbf{1}$	0	0	0	0	1	-1	-2	-1	1
w_2	$\frac{y^2-y}{2}$	0	$\mathbf{1}$	0	0	0	0	1	1	0	-1
w_3	$\frac{x^2-x}{2}$	0	0	$\mathbf{1}$	0	0	0	0	1	0	0
w_4	$\frac{y^2-x^2+y+x}{2}$	0	0	0	$\mathbf{1}$	0	0	0	0	1	-1
w_5	$\frac{-y^2+x^2+y+x}{2}$	0	0	0	0	$\mathbf{1}$	0	0	0	0	1

Keywords
Degroebnerization, Normal Form, Algebraic Statistics

References

[1] AUZINGER W.; STETTER H.J., *An Elimination Algorithm for the Computationof all Zeros of a System of Multivariate Polynomial Equations*, I.S.N.M. 86 (1988), 11–30, Birkhäuser

[2] ABBOTT, J.; BIGATTI, A.; KREUZER, M.; ROBBIANO, L., *Computing ideals of points*, J. Symbolic Comp. **30**,2000, 341–356.

[3] CERIA, M., *Bar Code for monomial ideals*, Journal of Symbolic Computation, Volume 91, March - April 2019, DOI: 10.1016/$j.jsc$.2018.06.012, 30-56.

[4] CERIA, M.; MORA, T.; VISCONTI, A. *Degroebnerization and its applications: a new approach for data modelling*, talk for MEGA2021, paper in preparation.

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

[6] LAUBENBACHER, R.; STIGLER, B., *Design of experiments and biochemical network inference* in Algebraic and Geometric Methods in Statistics. Eds: Gibilisco, Riccomagno, Rogantin, Wynn, Cambridge University Press (2008)

[7] LUNDQVIST, S., *Vector space bases associated to vanishing ideals of points*, Journal of Pure and Applied Algebra **214**(4), 309–321 (2010)

[8] MARINARI, M.G.; MÖLLER, 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)

[9] MORA T., *Solving Polynomial Equation Systems* 4 Vols., Cambridge University Press, I DOI: 10.1017/$CBO$9780511542831 (2003), II DOI: 10.1017/$CBO$9781107340954 (2005), III DOI: 10.1017/$CBO$9781139015998 (2015), IV DOI:10.1017/$CBO$9781316271902 (2016).

[10] MORA, T., *An FGLM-like algorithm for computing the radical of a zero-dimensional ideal.* Journal of Algebra and Its Applications, **17**(01) (2018).

[11] MORA, T., Robbiano, L. *Points in affine and projective spaces* In Computational Algebraic Geometry and Commutative Algebra, Cortona-91, **34**, 106-150. Cambridge University Press (1993).

[12] MORA T., slides available at http://www.dima.unige.it/∼morafe/SLIDES/TR8.pdf

[13] MORA T., slides available at http://www.dima.unige.it/∼morafe/SLIDES/SantiagoMacaulay.pdf

[14] MORA T., slides available at http://www.dima.unige.it/∼morafe/SLIDES/BondingUMI.pdf

[15] MOURRAIN B., A New Criterion for Normal Form Algorithms. In: Fossorier M.,

Imai H., Lin S., Poli A. (eds) Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. AAECC 1999. Lecture Notes in Computer Science, **1719**, Springer, Berlin, Heidelberg (1999)

[16] MOURRAIN B., *Bezoutian and quotient ring structure* J. Symb. Comp. **39** (2005), 397-415

[17] ONN, S.; STURMFELS, B. Cutting corners. Adv Appl Math **23(1)**:29–48 (1999).

[18] PISTONE G.; ROGANTIN M.P., *Indicator function and complex coding for mixed fractional factorial designs* Journal of Statistical Planning and Inference **138**,3, 787–802, 2008, Elsevier.

[19] PISTONE G.; RICCOMAGNO E., Rogantin M.P., *Methods in algebraic statistics for the design of experiments* in Optimal Design and Related Areas in Optimization and Statistics, 97–132, 2009, Springer

[20] ROBBIANO, L., *Gröbner bases and statistics.* In Gröbner Bases and Applications Buchberger, B. and Winkler, F. eds. (Cambridge, Cambridge University Press) 179-204 (1998).

[21] ROUILLIER F., *Solving Zero-Dimensional Systems Through the Rational Univariate Representation*, J. AAECC **9** (1999), 433–461

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic Geometry from an Algorithmic Point of View”*

De Nugis Groebnerialium 6: Rump, Ufnarovski, Zacharias

***Michela Ceria*[1], *Ferdinando Mora*[2]** [5919@unige.it]

[1] Dipartimento di Meccanica, Matematica e Management, Politecnico di Bari, Via Orabona 4, I-70125 Bari, Italy
[2] Dipartimento di Matematica, Università di Genova, Via Dodecaneso 35, 16146, Genova, Italy

Recently, Wolfgang Rump, in connection with [11], posed us the following question:

> Consider the ring $\mathbb{Z}\langle p, q, q' \rangle$ with generators p and q, q' and relations $qq' = q'q = 1$ and $pq - qp = p^2$. Thus $q' = q^{-1}$ $[\cdots]$. One easily shows that $(q + p)(q^{-1} - pq^{-2}) = 1$.
> My question: Is $q + p$ invertible? Does $px = 0$ imply that $x = 0$?

We easily gave an answer to all questions using the classical tecniques of Zacharias' canonical representation [12]. Unfortnately we made the unjustifiable ridiculous mistake of assuming that the given basis was Gröbner, while as Rump remarked “*note that $pq^2 - q^2p = 2pqp$ reduces $p^3 = (pp)p = p(pp)$ in two ways*”.

This gives a first intriguing Ufnarovski-like sequence [4,5,6,7,8] with coefficients in $\mathbb{Z}$: $G := \{f_i : i \in \mathbb{N} \setminus \{0\}\}$ with

$$f_1 = p^2 - pq + qp, f_2 = 2pqp - pq^2 + q^2p,$$
$$f_3 = 3pq^2p - pq^3 + q^3p, \dots, f_n = npq^{n-1}p - pq^n + q^np, \dots;$$

it would be just sufficient to consider this sequence under any term-ording on $\langle p, q, q^{-1} \rangle$ for which

$$\deg_p(\tau_1) < \deg_p(\tau_2) \implies \tau_1 < \tau_2, \text{ for each } \tau_1, \tau_2 \in \langle p, q, q^{-1} \rangle \tag{1}$$

and discuss the posed questions in this Ufnarovski-like setting, as we will do, to show the power of Zacharias' results for a Buchberger Theory (and practice) of effective associative rings [1,2,9,10].

However, the principal ideal $\mathbb{I}(p^2 - pq + qp) \subset \mathbb{Z}\langle p, q, q^{-1}\rangle$ introduced by Rump [11] could have a better Gröbner basis as can be shown by the first most elementary S-polynomials, if we could assume the existence of a term-ordering satsfying $pq^3p > pqpq^2$ and $pq^3p > q^2pqp$:

$$\begin{array}{rcl} f_2qp - qpf_2 & \rightarrow & -\mathbf{2pq^3p} + pqpq^2 + q^2pqp =: g \\ f_4 + 2g & \rightarrow & 0 \end{array}$$

If such a term-ordering does not exist, this kind of study could potentially lead to a study on noncommutative *marked bases* [3].

Keywords
Zacharias representation, Ufnarovski sequence, Yang-Baxter equation

References

[1] M. CERIA; T. MORA, Buchberger–Zacharias theory of multivariate Ore extensions. *J. Pure Appl. Algebra* **221**(12), first 2974–3026 (2017).
[2] M. CERIA; T. MORA, Buchberger–Weispfenning theory for effective associative ring. *Journal of Symbolic Computation* **83**, 112–146 (2017).
[3] F. CIOFFI; M. ROGGERO, *Flat families by strongly stable ideals and a generalization of Gröbner bases*, Journal of Symbolic Computation **46** (9), 1070-1084
[4] S. COJOCARU; V. UFNAROVSKI, Noncommuatative Gröbner basis, Hilbert series, Anick's resolution and BERGMAN under MS-DOS. *Computer Science Journal of Moldova* **3** 24–39 (1995).
[5] E. GREEN; T. MORA; V. UFNAROVSKI, The non-commutative Gröbner freaks. In *Symbolic rewriting techniques*, M. Bronstein, J. Grabmeier, V. Weispfenning (eds.), 93–104. Birkhäuser, Basel, 1998.
[6] J. MÅNSSON, On the computation of Hilbert series and Poincare series for algebras with infinite Gröbner bases. *Computer Science Journal of Moldova* **8**(1) 42–63 (2000).
[7] J. MÅNSSON; P. NORDBECK, A generalized Ufnarovski graph. *Applicable Algebra in Engineering, Communication and Computing* **16**(5), 293–306 (2005).
[8] K. MÅRTENSSON, *An algorithm to detect regular behaviour of binomial Gröbner Basis rational language*. Master's Thesis, Lund University, 2006.
[9] T. MORA, Zacharias representation of effective associative rings. *Journal of Symbolic Computation* **99**, 147–188 (2020).
[10] B. NGUEFACK; E. POLA, Effective Buchberger-Zacharias-Weispfenning theory of skew polynomial extensions of restricted bilateral coherent rings. *Journal of Symbolic Computation* **99**, 50–107 (2020).
[11] W. RUMP, *Degenerate involutive set-theoretic solutions to the Yang-Baxter equation*. prerint, 2021.
[12] G. ZACHARIAS, *Generalized Gröbner bases in commutative polynomial rings.*. Bachelor Thesis, MIT Dept. of Comp. Sci, 1978.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Algebraic Geometry from an Algorithmic Point of View"*

Cotangent Spaces and Separating Re-embeddings

Le Ngoc Long[1]***, Martin Kreuzer***[1]***, Lorenzo Robbiano***[2] [Ngoc-Long.Le@uni-passau.de]

[1] Fakultät für Informatik und Mathematik, Universität Passau, D-94030 Passau, Germany
[2] Dipartimento di Matematica, Università di Genova, Via Dodecaneso 35, I-16146 Genova, Italy

Given an affine scheme $\mathbb{X}$ embedded in an affine space $\mathbb{A}^n_K$ over a field K, it is a natural question to ask whether $\mathbb{X}$ can be embedded into an affine space of lower dimension. For instance, a classical result in algebraic geometry says that a smooth affine variety of dimension d over an infinite field K can be embedded into $\mathbb{A}^{2d+1}_K$. This was generalized by V. Srinivas to the non-smooth case in [6]. The method to prove these results is to start with an embedding $\mathbb{X} \to \mathbb{A}^n_K$ into a high-dimensional affine space and then to apply general linear projections which re-embed $\mathbb{X}$, i.e., which define isomorphisms on $\mathbb{X}$. Partial solutions to the above problem can be found in many papers. Among them, it is worth mentioning [2] and [3] where an approach of algebraic nature is used.

Although the general problem of finding the minimal number of algebra generators of an affine K-algebra seems to be very hard, it turns out to be possible to re-embed some affine schemes in much lower dimensional affine spaces using linear projections based on *separating indeterminates*. Let us write $\mathbb{X} = \operatorname{Spec}(P/I)$, where $P = K[x_1, \ldots, x_n]$ is a polynomial ring over K and I is an ideal in P. If a polynomial in I is of the form $f = z - g$ where the indeterminate $z \in \{x_1, ..., x_n\}$ does not divide any term in the support of g, one can eliminate z from the polynomials in I in an obvious way. To eliminate several indeterminates at a time (as well as to find re-embeddings of $\mathbb{X}$, i.e., presentations $P/I \cong P'/I'$ such that P' is a polynomial ring in fewer indeterminates), we needs polynomials f_i in the ideal I which are *coherently separating* in the sense defined below. The possible numbers of such sets of polynomials are shown to be governed by the *Gröbner fan* of I which was first introduced and studied in [5] and is hard to compute in general. The main advantage of such re-embeddings is that they do not involve generic changes of coordinates. Can we reach the embedding dimension, i.e., the smallest dimension of the ambient space in this way? In general, this is impossible, because the optimal re-embedding may not be achieved via linear projections. However, the dimension of the cotangent space of P/I at a K-linear maximal ideal is a lower bound for the embedding dimension, and if we find coherently separating polynomials corresponding to this bound, we know that we have determined the embedding dimension of P/I and found an optimal re-embedding.

In this talk I will firstly discuss about the computation of the tangent and cotangent space of

P/I at a K-linear maximal ideal which can be achieved efficiently using any set of generators of I. Then I present how to find optimal separating re-embeddings of $\mathbb{X}$. More precisely, given a set of distinct indeterminates $Z = \{z_1, ..., z_s\}$ in $X = \{x_1, ..., x_n\}$, we say that a set of polynomials $f_1, ..., f_s \in I$ is *coherently Z-separating* if each f_i is of the form $f_i = z_i - g_i$ with $g_i \in P$ such that z_i divides neither a term in the support of g_i nor in the support of f_j for $j \neq i$. We show that the existence of a coherently Z-separating set $\{f_1, ..., f_s\}$ is equivalent to the existence of a Gröbner basis of I of a very special shape. This allows us to define an isomorphism $\Phi : P/I \to \hat{P}/(I \cap \hat{P})$, where $\hat{P} = K[X \setminus Z]$ has fewer indeterminates. Thus the map Φ corresponds to a re-embedding of $\mathbb{X} = \mathrm{Spec}(P/I)$ into a lower-dimensional affine space. We call it the *Z-separating re-embedding* of $\mathbb{X}$ (or of I).

To get an optimal separating re-embedding of $\mathbb{X}$, we indicate that the sets Z for which a coherently Z-separating set of polynomials in I exists correspond to the sets of leading indeterminates of a reduced Gröbner basis of I. By computing the Gröbner fan of I, i.e., the set of marked reduced Gröbner bases of I, we get a finite set Σ of possible choices of Z, and consequently, a Z-separating re-embedding of $\mathbb{X}$ is optimal if and only if $Z \in \Sigma$ is an element such that $\#Z$ is maximal. For example, consider $P = \mathbb{Q}[x, y, z]$ and $\mathbb{X} = \mathrm{Spec}(P/I)$ with $I = \langle f_1, ..., f_6\rangle$, where $f_1 = x^2 - y$, $f_2 = xy - x - z$, $f_3 = y^2 + z^2 + 2x + y + 2z$, $f_4 = xz + z^2 + 2x + 2y + 2z$, $f_5 = yz + z^2 + 3x + 3y + 3z$, and $f_6 = z^3 + z^2 - 5x - 5y - 5z$. Using the computer algebra system CoCoA [1], we find $\Sigma = \{\{x\}, \{y\}, \{z\}, \{z, y\}\}$ and a marked reduced Gröbner basis of I associated to $Z = \{y, z\}$ is given by

$$\overline{G} = \{(y, y - x^2), (z, z - x^3 + x), (x^5, x^5 - x^4 + 2x^2)\}.$$

Then an optimal separating re-embedding of $\mathbb{X}$ with respect to Z is the map $\Phi : P/I \to \mathbb{Q}[x]/I'$ given by $x + I \mapsto x + I'$, $y + I \mapsto x^2 + I'$, and $z + I \mapsto x^3 - x + I'$, where $I' = \langle x^5 - x^4 + 2x^2\rangle$. In this case Φ also yields an optimal re-embedding of $\mathbb{X}$.

Next, it is natural to look at whether a given optimal Z-separating re-embedding of $\mathbb{X}$ yields an optimal re-embedding of $\mathbb{X}$. We show that the dimension d of the cotangent space of P/I at a K-linear maximal ideal is less than or equal to the embedding dimension of P/I. Therefore, the condition $d = n - \#Z$ gives us a criterion for checking the mentioned problem. The results in this talk are partially given in the paper [4].

Keywords
cotangent space, embedding dimension, affine scheme, Gröbner basis, Gröbner fan

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] C. Bertone; F. Cioffi, The close relation between border and Pommaret marked bases. Collectanea Mathematica, `doi:10.1007/s13348-021-00313-w` (2020).

[3] G. Ferrarese; M. Roggero, Homogeneous varieties for Hilbert schemes. *Int. J. Algebra* **3** (11), 547–557 (2009).

[4] M. Kreuzer; L.N. Long; L. Robbiano, Cotangent spaces and separating re-embedding. *J. Algebra Appl.*, (to appear 2021).

[5] T. Mora; L. Robbiano, The Gröbner fan of an ideal. *J. Symb. Comput.* **6**, 183–208 (1988).

[6] V. Srinivasan, On the embedding dimension of an affine variety. *Math. Ann.* **289**, 125–132 (1991).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic Geometry from an Algorithmic Point of View”*

Relative Gröbner and Involutive Bases for Ideals in Quotient Rings

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

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

Gröbner bases, introduced by Buchberger in his thesis [2], provide a powerful computational tool for analysing the properties of ideals in the polynomial ring $\mathcal{P} = K[x_1, \ldots, x_n]$ over a field K. In particular, a well-known construction by Schreyer [10] uses Gröbner bases to construct free resolutions of finitely generated $\mathcal{P}$-modules. Involutive bases are Gröbner bases with additional combinatorial properties introduced by Gerdt and Blinkov [3]. An overview over their theory can be found in [11]. They arise via a restriction of the usual divisibility relation of monomials to an involutive division.

In our work [5], we extend the concepts of Gröbner bases and involutive bases to ideals in and modules over quotient rings $\mathcal{P}/I$, where $I \lhd \mathcal{P}$ is an ideal. For Gröbner bases, such an extension is not new [1]. La Scala and Stillman [7] sketched the necessary theoretical background and implemented procedures in MACAULAY2 not only for computing Gröbner bases, but also for free resolutions. Mora developed a general framework for the analysis of rings for which classical Gröbner bases theory also carries over to their factor rings [8].

It is well-known that any ideal $\overline{J} \lhd \mathcal{P}/I$ can be identified with an ideal $I \subseteq J \lhd \mathcal{P}$. Given a monomial ordering $\prec$ on $\mathcal{P}$, a Gröbner basis G of I and such an ideal J, we call a finite subset $H \subset J$ a *Gröbner basis of J for $\prec$ relative to I*, if $H \cup G$ is a Gröbner basis of J for $\prec$. This definition can be extended to submodules of the free $\mathcal{P}/I$-module $(\mathcal{P}/I)^m$ by using m copies of G, one for each module component. One can check whether a set $H \cup G$ is a relative Gröbner basis by computing normal forms of all its S-polynomials. Since G is by assumption a Gröbner basis of I, we ignore S-polynomials between elements of G. We call S-polynomials between an element of H and an element of G *A-polynomials* in analogy to the theory of Gröbner bases over principal ideal domains (cf. [9]) and use the terminology S-polynomials exclusively for those between elements of H. For computing relative Gröbner bases, we use a relative version of the Buchberger algorithm. Its efficiency can be enhanced by using adaptions of the well-known Buchberger criteria. Lastly, we obtain a relative version of the classical Schreyer theorem:

Theorem 1. *Let G be the reduced Gröbner basis of the ideal $I \lhd \mathcal{P}$ and let $H = \{h_1, \dots, h_r\}$ be a Gröbner basis of the ideal $J \supseteq I$ relative to I such that $\mathrm{NF}_G(H) = H$. Then, with respect to a suitable ordering, the syzygies induced by the S- and A-polynomials of H and G form a Gröbner basis of the relative syzygy module $\mathrm{Syz}_{\mathcal{P}/I}([h_1], \dots, [h_r])$ relative to I.*

Our theory of involutive bases in factor rings rests on the definition of the involutive divisions in this context. Guided by the distinction between S- and A-polynomials, we choose the following approach: An *involutive division relative to a monomial ideal I* has to satisfy exactly the same axioms as usually – but only outside of I. Assume that, to a monomial $\mathbf{x}^\mu$ in a finite set H of monomials, some involutive division L assigns the multiplicative variables $L(\mathbf{x}^\mu, H)$; its *relative involutive cone* is $\mathcal{C}_{L,H,I}(\mathbf{x}^\mu) = \mathbf{x}^\mu \cdot K[L(\mathbf{x}^\mu, H)] \setminus I$. If L is a classical involutive division and $I \lhd \mathcal{P}$ is a monomial ideal, then an involutive division L_I relative to I is defined by $x_i \in L_I(\mathbf{x}^\mu, H)$, if and only if either $x_i \in L(\mathbf{x}^\mu, H)$ or $x_i \mathbf{x}^\mu \in I$.

Given two monomial ideals $I \subset J$, a finite set H of monomials not contained in I is a *weak L-involutive basis of J relative to I*, if the residue classes modulo I of $\bigcup_{\mathbf{x}^\mu \in H} \mathcal{C}_{L,H,I}(\mathbf{x}^\mu)$ are a basis of J/I as a K-linear space. It is a *(strong) L-involutive basis of J relative to I*, if in addition the relative involutive cones are disjoint. Given two polynomial ideals $I \subset J$, a monomial ordering $\prec$ and a Gröbner basis G of I for $\prec$, a finite set $H \subset J \setminus I$ satisfying $\mathrm{NF}_G(H) = H$ is a *weak L-involutive basis of J relative to I for $\prec$*, if $\mathrm{lm}(H)$ is a weak L-involutive basis of $\mathrm{lm}(J)$ relative to $\mathrm{lm}(I)$. The basis H is *strong*, if additionally, the leading monomials of the elements of H are distinct and form a strong L-involutive basis of $\mathrm{lm}(J)$ relative to $\mathrm{lm}(I)$. For the computation of relative involutive bases, we augment the usual involutive completion algorithm [3], [11, Algo. 4.5] by a treatment of the A-polynomials. We always consider A-polynomials before non-multiplicative prolongations and use non-involutive reductions for them. Also the TQ algorithm for the construction of minimal involutive bases [4], [11, Algo. 4.6] can be adapted to the relative case.

Theorem 2. *Let $I \subseteq J \lhd \mathcal{P}$ be polynomial ideals and let L be an involutive division relative to I. Let $H \subset J \setminus I$ be a strong L-involutive basis of J relative to I. Then, the cones*

$$\mathcal{C}_{L,\mathrm{lm}(H),\mathrm{lm}(I)}(h) = \left\langle \mathrm{NF}_I(\mathbf{x}^\rho h) \mid \mathbf{x}^\rho \mathrm{lm}(h) \in \mathcal{C}_{L,\mathrm{lm}(H),\mathrm{lm}(I)}(\mathrm{lm}(h)) \right\rangle_K \tag{0.1}$$

induce the following decomposition of the K-linear space J:

$$J = \left(\bigoplus_{h \in H} \mathcal{C}_{L,\mathrm{lm}(H),\mathrm{lm}(I)}(h) \right) \oplus I\,. \tag{0.2}$$

We prove an involutive version of Theorem 1 under some assumptions on the used relative involutive division. These assumptions are satisfied for the relative Pommaret division, but not for the relative Janet division.

The Pommaret division is of great interest because of its close relation to the important notion of quasi-stable ideals. We extend now this relation to the relative case. For a monomial $\mathbf{x}^\mu$, its class is defined as $\mathrm{cls}(\mathbf{x}^\mu) = \min\{i \mid \mu_i > 0\}$. Given two monomials ideals $I \subset J$, we say that J is *quasi-stable relative to I*, if for any monomial $\mathbf{x}^\mu \in J \setminus I$ with $\mathrm{cls}(\mathbf{x}^\mu) = k$ and any index $k < i \leq n$ an exponent $s \geq 0$ exists such that either $x_i^s \mathbf{x}^\mu \in I$ or $x_i^s \mathbf{x}^\mu / x_k \in J$.

Theorem 3. *The monomial ideal $J \supset I$ is quasi-stable relative to I, if and only if it possesses a finite Pommaret basis relative to I.*

Given two polynomial ideals $I \subset J$, we say that J is *in quasi-stable position relative to* I for a monomial ordering $\prec$, if $\mathrm{lm}(J)$ is quasi-stable relative to $\mathrm{lm}(I)$. We extend the results in [6] to an algorithm that computes deterministically a linear change Φ of coordinates such that $\Phi(J)$ is in quasi-stable position relative to $\Phi(I)$. A modified version of this algorithm even transforms also I into quasi-stable position simultaneously.

Acknowledgement

The research of the first author was in part supported by a grant from IPM (No. 1400130214).

Keywords
Polynomial rings, quotient rings, ideals, Gröbner bases, syzygy module, involutive bases, quasi-stable ideals

References

[1] T. Becker and V. Weispfenning. *Gröbner bases: a computational approach to commutative algebra. In cooperation with Heinz Kredel.*, volume 141. New York: Springer-Verlag, 1993.

[2] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, Universität Innsbruck, 1965.

[3] V. P. Gerdt and Y. A. Blinkov. Involutive bases of polynomial ideals. *Math. Comput. Simul.*, 45(5-6):519–541, 1998.

[4] V. P. Gerdt and Y. A. Blinkov. Minimal involutive bases. *Math. Comput. Simul.*, 45(5-6):543–560, 1998.

[5] A. Hashemi, M. Orth, and W. M. Seiler. Relative Gröbner and involutive bases for ideals in quotient rings. *Math. Comput. Sci.*, 2021. Accepted for publication.

[6] A. Hashemi, M. Schweinfurter, and W. M. Seiler. Deterministic genericity for polynomial ideals. *J. Symb. Comput.*, 86:20–50, 2018.

[7] R. La Scala and M. Stillman. Strategies for computing minimal free resolutions. *J. Symb. Comput.*, 26(4):409–431, 1998.

[8] T. Mora. De Nugis Groebnerialium 4: Zacharias, Spears, Möller. In *Proc. Intern. Symp. Symbolic Algebraic Computation, ISSAC 2015, Bath, United Kingdom*, pages 191–198. New York, NY: ACM Press, 2015.

[9] G. H. Norton and A. Sălăgean. Strong Gröbner bases for polynomials over a principal ideal ring. *Bull. Aust. Math. Soc.*, 64(3):505–528, 2001.

[10] F.-O. Schreyer. Die Berechnung von Syzygien mit dem verallgemeinerten Weierstrass'schen Divisionssatz. Master's thesis, University of Hamburg, Germany, 1980.

[11] W. M. Seiler. *Involution. The formal theory of differential equations and its applications in computer algebra.* Berlin: Springer, 2010.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *““Algebraic Geometry from an algorithmic point of view”*

Computational VGIT for Complete Intersections and a Hyperplane

Theodoros Papazachariou[1] [tp19470@essex.ac.uk]

[1] Department of Mathematical Sciences, University of Essex, Colchester, United Kingdom

A Fano variety X, is a projective variety embedded in some projective space $\mathbb{P}^n$ with an ample anti-canonical bundle $-K_X$. For hypersurfaces of degree d and complete intersections of k hypersurfaces of degree d this is achieved if $d \leq n$ and $kd \leq n$ respectively. The study of Fano varieties is an integral part in many of the subfields of algebraic geometry, as they can act as building blocks for other varieties, and is a fast growing, although few results are known about their classification. Recent efforts to study Fano varieties have focused on the creation of moduli spaces in order to achieve a classification.

Geometric invariant theory (GIT), pioneered by Mumford [1], based on Hilbert's classical invariant theory, is an effective method to study the construction of quotients by group actions in algebraic geometry, which in turn give rise to moduli spaces. Consider a projective variety $X \hookrightarrow \mathbb{P}^n$ over $\mathbb{C}$, let L be an ample line bundle on X and let G be a reductive group acting on X. We define

$$k[X]^G \colon = \bigoplus_{m\geq 0} H^0(X, L^{\otimes m})^G$$

to be all the invariant elements of $k[X]$ under the action of G, which is finitely generated. We also define the set of semi-stable points, X^{ss}, which consist of all points $x \in X$ such that there exists some m and invariant section $s \in H^0(X, L^{\otimes m})$ such that $s(x) \neq 0$. Under this definition X^{ss} is an open subset of X and the map ϕ restricts to a well defined categorical quotient [2]

$$\phi\colon X^{ss} \to X /\!\!/ G \colon = \mathrm{Proj}(k[X]^G).$$

Extending this type of thinking, we define a set of stable points X^s as the set of $x \in X^{ss}$, with the orbit $G \cdot x$ closed, and finite stabilizer $\mathrm{Stab}(x)$. Under this definition X^s is an open subset of X, with $X^s \subseteq X^{ss} \subseteq X$ and the map ϕ restricts to a well defined geometric quotient

$$\phi\colon X^s \to X/G.$$

The main goal of GIT is to describe the good loci X^s, X^{ss}, X^{ps}, where X^{ps} are the polystable points, semi-stable points with closed orbits. The categorical and (closure of) geometric quotients give rise to a well defined moduli stack $\mathcal{M}^{GIT}$ and moduli space M^{GIT} respectively.

The method of study to detect stable, semi-stable and polystable points is via the Hilbert-Mumford numerical criterion. Consider non-trivial homomorphisms called 1 parameter subgroups (1-PS) $\lambda\colon \mathbb{G}_m \to G$. The action of G on X extends to an action of $\mathbb{G}_m$ on X via the 1-PS, and the numerical criterion [3] states that

1. $x \in X$ is semi-stable if and only if $\lim_{t\to 0} \lambda(t) \cdot x \neq 0$ for all 1-PS $\lambda\colon \mathbb{G}_m \to G$;
2. $x \in X$ is stable if and only if $\lim_{t\to 0} \lambda(t) \cdot x$ does not exist for all 1-PS $\lambda\colon \mathbb{G}_m \to G$;

An interesting phenomenon occurs when the Picard rank of X is greater than 1. In this case, the categorical quotient depends on the linearization L. In particular, if $\dim \mathrm{Pic}(X) = 2$, $L \cong \mathcal{O}(a, b)$, and one obtains a finite wall-chamber decomposition where the stability conditions are the same for each wall/chamber $t\colon = \frac{b}{a}$ [4], [5].

More formally, when $\dim \mathrm{Pic}(X) = 1$, $L \cong \mathcal{O}(a)$ for $a \in \mathbb{Z}$, and since the choice of linearization does not change whether we choose the line bundle L or the line bundle L^r for some $r \in \mathbb{Z}$, there exists only one GIT quotient $X /\!\!/ G = X /\!\!/_L G$, where $L = \mathcal{O}(1)$. In the situation where $\dim \mathrm{Pic}(X) = 2$, $L \cong \mathcal{O}(a, b)$ and the GIT quotient is denoted by $X /\!\!/_L G$, to demonstrate that there is a dependency on the choice of linearization. Two different quotients $X /\!\!/_L G$ and $X /\!\!/_M G$ will not be isomorphic unless $M = L^r$ for some r. Also setting $t = \frac{b}{a}$, and recognising that the quotient depends only on t, we write $X /\!\!/_t G$.

The important discovery by Dolgachev- Hu [4] and Thaddeus [5] is that there exist intervals where these quotients are isomorphic. In particular, there exist intervals $[t_i, t_{i+1}]$ such that $X /\!\!/_t \cong X /\!\!/_{t'} G$ for all $t, t' \in (t_i, t_{i+1})$, but $X /\!\!/_t \ncong X /\!\!/_{t_i} G \ncong X /\!\!/_{t_{i+1}} G$. The open intervals (t_i, t_{i+1}) are called chambers, and the endpoints of the interval t_i, t_{i+1} are called walls. An important property of these walls and chambers is that the two different quotients $X /\!\!/_t G$ and $X /\!\!/_{t_{i+1}} G$ are connected via a map which is constructed via flips and flops. These morphisms are called wall-crossing morphisms, and although hard to describe carry important birational geometric properties. Another important property is that the number of walls/ chambers is finite; there exists a final wall t_n and a chamber (t_{n-1}, t_n) so the number of different quotients is finite. This particular "flavour" of GIT is called Variational GIT (VGIT) and has been an item of study recently for algebraic geometers [6], [7].

In this talk we will describe a computational algorithm used to find the unstable (not-semistable) and not stable points for a pair (X, H) where X is a complete intersection of k hypersurfaces of degree d and H is a hyperplane in $\mathbb{P}^n$, under the action of $\mathrm{SL(n+1)}$ in the particular case of Fano varieties. We will also demonstrate in a specific example how the above can lead to the description of the moduli space M^{GIT}.

Classically the way to study the complete intersection of k hypersurfaces of degree d has been through the study of the Grassmanian

$$\mathrm{Gr}\left(k, \binom{n+d}{d}\right).$$

As such, in the case of pairs (X, H) we aim to study the quotient

$$\mathcal{R} /\!\!/ \mathrm{SL}(n+1)\colon = \mathrm{Gr}\left(k, \binom{n+d}{d}\right) \times \mathbb{P}^n /\!\!/ \mathrm{SL}(n+1)$$

computationally. Since $\dim \mathrm{Pic}(\mathcal{R}) = 2$ this lies in the field of VGIT and we expect a finite wall-chamber decomposition. Note, that the first wall $t = 0$ corresponds to the GIT quotient

$$\mathrm{Gr}\left(k, \binom{n+d}{d}\right) /\!\!/ \mathrm{SL}(n+1)$$

which parametrizes complete intersections. We study the above using the Hilbert-Mumford. The first step is to show there is a finite set of one-parameter subgroups $P_{n,d,k}$ which destabilize pairs (X, H) irregardless of wall, which can also be computed algorithmically via a computer program.

Using this we also show that there exist maximal (semi-)destablising families for each wall, that parametrise unstable and non-stable pairs, which can also be found computationally. We further show that the maximal wall can be computed using only the initial parameters n, k, d, and we demonstrate some results particular to Fano varieties regarding stability conditions.

We close the talk by demonstrating a particular example of the complete intersection of two quadrics in $\mathbb{P}^3$ which we obtained via the Sagemath program we have developed, which will soon appear as a completed package.

Keywords
Geometric Invariant Theory, Fano varieties, Complete intersections

References

[1] D. Mumford; J. Fogarty; F. C. Kirwan, *Geometric Invariant Theory*.Springer, 1994
[2]V. Hoskins, *Moduli Problems and Geometric Invariant Theory*. https://userpage.fu-berlin.de/hoskins/M15_Lecture_notes.pdf, 2015.
[3] S. Mukai, *An Introduction to Invariants and Moduli Theory*.Cambridge University Press, 2003.
[4]I. Dolgachev; Y. Hu., Variation of geometric invariant theory quotients. *Publications mathématiques de l'IHÉS* **87**(03) (1994).
[5]M. Thaddeus, Geometric invariant theory and flips. *J. Amer. Math. Soc* **6**, 691–723 (1996).
[6]R. Laza; K. G. O'Grady, GIT versus Baily-Borel compactification for quarticK3surfaces. *Geometry of moduli* **14** of *Abel Symp.*, 217–283 (2018).
[7]P. Gallardo; J. Martinez-Garcia, Variations of geometric invariant quotients forpairs, a computational approach. *Proceedings of the American Mathematical Society* **146**(6), 2395–2408 (2018).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Algebraic Geometry from an algorithmic point of view"*

Finite quotients of surface braid groups and double Kodaira fibrations: an algorithmic approach

Francesco Polizzi[1] [francesco.polizzi@unical.it],

[1] Dipartimento di Matematica e Informatica, Università della Calabria, Arcavacata di Rende (Cosenza), Italy

A *Kodaira fibration* is a smooth, connected holomorphic fibration $f_1 \colon S \to B_1$, where S is a compact complex surface and B_1 is a compact complex curve, which is not isotrivial (this means that not all its fibres are biholomorphic to each others). The genus $b_1 := g(B_1)$ is called the *base genus* of the fibration, whereas the genus $g := g(F)$, where F is any fibre, is called the *fibre genus*. If a surface S is the total space of a Kodaira fibration, we will call it a *Kodaira fibred surface*. For every Kodaira fibration we have $b_1 \geq 2$ and $g \geq 3$. Moreover, since the fibration is smooth, the condition on the base genus implies that S contains no rational or elliptic curves; hence it is minimal and, by the sub-additivity of the Kodaira dimension, it is of general type, hence algebraic.

Examples of Kodaira fibrations were originally constructed (independently) by Kodaira and Atiyah in order to show that, unlike the topological Euler characteristic, the signature σ of a real manifold is not multiplicative for fibre bundles. In fact, every Kodaira fibred surface S satisfies $\sigma(S) > 0$, see for example the introduction of [3], whereas $\sigma(B_1) = \sigma(F) = 0$, and so $\sigma(S) \neq \sigma(B_1)\sigma(F)$.

A *double Kodaira surface* is a compact complex surface S, endowed with a *double Kodaira fibration*, namely a surjective, holomorphic map $f \colon S \to B_1 \times B_2$ yielding, by composition with the natural projections, two Kodaira fibrations $f_i \colon S \to B_i$, $i = 1, 2$, see [2].

The purpose of this talk is to give an account of recent results concerning the construction of some double Kodaira fibrations by means of group-theoretical methods. Let us start by introducing the needed terminology. Let $b \geq 2$ and $n \geq 2$ be two positive integers, and let $\mathsf{P}_2(\Sigma_b)$ be the pure braid group on two strands on a closed Riemann surface of genus b. We say that a finite group G is a *pure braid quotient* of type (b, n) if there exists a group epimorphism

$$\varphi \colon \mathsf{P}_2(\Sigma_b) \to G \tag{1}$$

such that $\varphi(A_{12})$ has order n, where A_{12} is the braid corresponding, via the isomorphism $\mathsf{P}_2(\Sigma_b) \simeq \pi_1(\Sigma_b \times \Sigma_b - \Delta)$, to the homotopy class in $\Sigma_b \times \Sigma_b - \Delta$ of a loop in $\Sigma_b \times \Sigma_b$

“winding once" around the diagonal Δ. Since A_{12} is a commutator in $\mathsf{P}_2(\Sigma_b)$ and $n \geq 2$, it follows that every pure braid quotient is a non-abelian group.

By Grauert-Remmert’s extension theorem and Serre’s GAGA, the existence of a pure braid quotient as in (1) is equivalent to the existence of a Galois cover $\mathbf{f}\colon S \to \Sigma_b \times \Sigma_b$, branched over Δ with branching order n. After Stein factorization, this yields in turn a double Kodaira fibration $f\colon S \to \Sigma_{b_1} \times \Sigma_{b_2}$.

We show that G is a pure braid quotient of type $(b,\, n)$ if and only if it admits a special system of generators, that we call a *diagonal double Kodaira structure* of type $(b,\, n)$ [4]. This allows us to “detopologize" the problem of constructing double Kodaira fibrations, by transforming it into a combinatorial-algebraic one (namely, the existence of diagonal double Kodaira structures on a given finite group), that, in principle, we can hope to solve by using computational methods.

In fact, we are able to prove that, if a finite group G admits a diagonal double Kodaira structure, then $|G| \geq 32$, and equality holds if and only if G is extra-special.

As a geometrical application of this algebraic result, we construct two 3-dimensional families of double Kodaira fibrations $f\colon S \to \Sigma_2 \times \Sigma_2$ having signature 16. To the best of our knowledge, these are the first positive-dimensional families of Kodaira fibrations with small signature that appear in the literature (some sporadic examples with the same signature were previously constructed in [3]).

Furthermore, for all the surfaces S in these families, we show that

$$H_1(S,\, \mathbb{Z}) = \mathbb{Z}^8 \oplus (\mathbb{Z}_2)^4.$$

From this, we deduce that they are *maximal* in the sense of [1], and we get information about the monodromy of the two Kodaira fibrations $f_i\colon S \to \Sigma_2$.

Part of our calculations were originally carried out by using the Computer Algebra Software `GAP4` [6]. The main idea behind our computations is to systematically look for diagonal double Kodaira structures on groups of small order, and to check that there is none if $|G| < 32$. Before doing this, we use some group theory in order to reduce the number of cases to analyse. More precisely, we show that, if a non-abelian finite group G is a CCT-group, (namely, if commutativity is a transitive relation on the set of non-central elements), then G admits no diagonal double Kodaira structures. It turns out that CCT groups are of historical importance in the context of classification of finite simple groups, and that there are precisely eight groups G with $|G| \leq 32$ that are not in this class, namely S_4 and seven groups of order 32. So, it only remains to check the existence of diagonal double Kodaira structures in these eight groups, a purely combinatorial problem that can be attacked by brute force via `GAP4`. The output is that the structures are only found in the two groups whose `GAP4` labels are $G(32,\, 49)$ and $G(32,\, 50)$, which are precisely the two extra-special groups of order 32.

These results have been obtained in collaboration with P. Sabatino, see the recent preprint [5].

Keywords
Surface braid groups, extra-special groups, Kodaira fibrations

References

[1] C. Bregman: On Kodaira fibrations with invariant cohomology, arXiv:1811.00584 (2018).
[2] F. Catanese: Kodaira fibrations and beyond: methods for moduli theory, *Japan. J. Math.* **12** (2017), no. 2, 91–174.
[3] J. A. Lee, M. Lönne, S. Rollenske: Double Kodaira fibrations with small signature, *Internat. J. Math.* **31** (2020), no. 7, 2050052, 42 pp.
[4] F. Polizzi: Diagonal double Kodaira structures on finite groups, arXiv:2002.01363 (2020). To appear in the *Proceedings of the 2019 ISAAC Congress* (*Aveiro, Portugal*).
[5] F. Polizzi, P. Sabatino: Diagonal double Kodaira fibrations with minimal signature, arXiv:2102.04963 (2021).
[6] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.11.1* (2021).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic geometry from an algorithmic point of view”*

Poincaré polynomials for some Schubert varieties

Carmine Sessa[1] [carmine.sessa2@unina.it]

[1] Dipartimento di Matematica e Applicazioni "Renato Caccioppoli", Università degli Studi di Napoli "Federico II", Naples, Italy

One of the most studied objects in algebraic geometry is very likely to be Grassmannians: for any pair of nonnegative integers $k < l$, $\mathbb{G}_k(\mathbb{C}^l)$ is the variety whose points are the k-vector subspaces of $\mathbb{C}^l$. Among all its properties, we know that their cohomology rings are generated by fundamental classes of particular subvarieties: the so-called Schubert varieties. The study of such spaces led to important discoveries in several branches of Mathematics and, in particular, it was proved [2, §6] that the coefficients of the Kazhdan-Lusztig polynomials are the dimensions of the stalks of the cohomology sheaves of intersection complexes of Schubert varieties. Although algorithms for the computation of such polynomials are available, we would like to find a new one by means of a geometric approach; namely, by virtue of suitable resolution of singularities (a proper morphism $f : \tilde{V} \to V$ is said to be a *resolution of singularities* if $\tilde{V}$ is smooth and there is a Zariski open dense subset U of V such that $f : f^{-1}(U) \to U$ is an isomorphism).

Let us begin with special Schubert varieties. Such spaces admit a Whitney stratification given by subvarieties (see Δ_p below) which are special Schubert varieties, as well. Apart from the fact that a suitable decomposition of the Schubert variety is required in the definition of the category of perverse sheaves and in related theorems, the existence of such a stratification allows us to prove our results by induction on the number of strata. Schubert varieties with two strata were studied in [7], while, in [3], we considered special Schubert varieties with an arbitrary number of strata. For any 4-tuple of integers i, j, k, l such that $0 < i < k \leq j < l$ and $r = k - i < l - j = c$ and for any fixed $F \in \mathbb{G}_j(\mathbb{C}^l)$, we call $\mathcal{S} = \{V \in \mathbb{G}_k(\mathbb{C}^l) : \dim(V \cap F) \geq i\}$ a *special Schubert variety*. As it is well known, $\mathcal{S}$ admits two standard resolutions: a small resolution $\xi : \mathcal{D} \to \mathcal{S}$ (that is, for any $\alpha > 0$, $\operatorname{codim}\{V \in \mathcal{S} : \dim \xi^{-1}(V) \geq \alpha\} > 2\alpha$) and a (usually) non-small one $\pi : \tilde{\mathcal{S}} \to \mathcal{S}$ [10, §3.4 and Exercise 3.4.10], where $\mathcal{D} = \{(V, U) \in \mathbb{G}_k(\mathbb{C}^l) \times \mathbb{G}_{j+r}(\mathbb{C}^l) : F + V \subseteq U\}$, $\tilde{\mathcal{S}} = \{(W, V) \in \mathbb{G}_i(F) \times \mathbb{G}_k(\mathbb{C}^l) : W \subseteq V\}$, ξ and π are projections onto the first and second factor, respectively.

By the celebrated *Decomposition theorem* [1, 4, 5, 11], in the bounded constructible derived category $D^b_c(\mathcal{S})$ of sheaves of $\mathbb{Q}$-vector spaces on $\mathcal{S}$ there is a decomposition

$$R\pi_* \mathbb{Q}_{\tilde{\mathcal{S}}}\,[n] \cong \bigoplus_{i \in \mathbb{Z}} {}^p\mathcal{H}^i(R\pi_* \mathbb{Q}_{\tilde{\mathcal{S}}}\,[n])\,[-i]\,, \tag{1}$$

where $R\pi_* \mathbb{Q}_{\tilde{\mathcal{S}}}$ represents the pushforward of an injective resolution of the constant sheaf $\mathbb{Q}_{\tilde{\mathcal{S}}}$, the functor $[n]$ is the translation by n functor [9, p.154] and ${}^p\mathcal{H}^i(R\pi_* \mathbb{Q}_{\tilde{\mathcal{S}}}\,[n])$ denotes the *perverse cohomology sheaves* [5, §1.5]. Furthermore, the perverse cohomology sheaves ${}^p\mathcal{H}^i(R\pi_*\mathbb{Q}_{\tilde{\mathcal{S}}}[n])$ are semisimple, i.e. direct sums of intersection cohomology complexes of semisimple local systems, supported in the smooth strata of $\mathcal{S}$.

In the paper [8], the summands involved in (1) are explicitly described. It turns out that the semisimple local systems involved in the decomposition are constant sheaves supported in the smooth strata of $\mathcal{S}$. In other words, the decomposition (1) takes the form

$$R\pi_*\mathbb{Q}_{\tilde{\mathcal{S}}} \cong \bigoplus_{p,q} IC^\bullet_{\Delta_p}[q]^{\oplus m_{pq}} \tag{2}$$

for suitable multiplicities $m_{pq} \in \mathbb{N}_0$ (computed in [8, Theorem 3.5]), where the strata $\Delta_p = \{V \in \mathbb{G}_k(\mathbb{C}^l) : \dim(V \cap F) \geq i_p = k - p + 1\}$ are special Schubert varieties, as well, and $IC^\bullet_{\Delta_p}$ denotes the *intersection cohomology complex* of Δ_p.

Following the same lines as in [7, §4], our main aim is to deduce a class of *local identities* as well as a class of *global identities* from isomorphism (2). The argument behind our local polynomial identity rests on the remark that *each summand of* (2) *is a direct sum of shifted trivial local systems* in $D^b_c(\mathcal{S})$, when restricted to the smooth part Δ^0_p of each stratum Δ_p. This fact follows by applying the Leray-Hirsch theorem (see [11, Theorem 7.33], [6, Lemma 2.5]) to the summands, which are described on Δ^0_p by means of suitable Grassmann fibrations. This implies that we are allowed to associate a Poincaré polynomial to each summand of (2), thus providing our local identity in the stratum Δ^0_p. As for the global polynomial identities, from (2) we deduce an isomorphism among the i-th hypercohomology spaces that leads to an equality of the corresponding Poincaré polynomials. Again, all summands are determined by means of Leray-Hirsch theorem as Poincaré polynomials of suitable Grassmann fibrations and this provides our global identity.

We also observe that an explicit inductive algorithm for the computation of the Poincaré polynomials of the intersection cohomology of Special Schubert varieties straightforwardly follows from our results

$$IH_{\Delta_p} = H_{\tilde{\Delta}_p} - \sum_{q=1}^{p-1} H_{\mathbb{G}_{p-q}(\mathbb{C}^{k-c})} IH_{\Delta_q} t^{2d_{pq}},$$

where H_X (respectively, IH_X) denotes the Poincaré polynomial of the cohomology (respectively, of the intersection cohomology) of a topological space X. Actually, although not explicitly stated in our work [3], from the proofs of our identities another algorithm arises, which computes the Poincaré polynomials of the local intersection cohomology complexes of special Schubert varieties. Indeed, for any $q < p$, the local polynomial identity can be expressed as follows

$$a_{pq} = b_{pq} + g_{pq} + \sum_{q<\tau<p} g_{p\tau} b_{\tau q}, \tag{3}$$

where a_{pq} is the Poincaré polynomial of the cohomology of a suitable Grassmannian, each $b_{\tau q}$ represents a Kazhdan-Lusztig polynomial and each g_{pq} is a symmetric polynomial with respect to a certain degree, say, m_{pq}. If we assumed that the polynomials g_{pq} and b_{pq} were unknown, the above equality would turn to an algorithm capable of computing them. Indeed, by means of the symmetry of g_{pq} and the fact that b_{pq} has degree less than m_{pq}, we deduce an iterative formula for computing g_{pq}. Now, (3) becomes an iterative algorithm for the computation of the polynomial b_{pq}, being the only remaining unknown. To sum up, for any $q < p$,

$$\begin{cases} g_{pq} = \tilde{U}_{pq}(R_{pq}) \\ b_{pq} = R_{pq} - g_{pq} \end{cases} \tag{4}$$

where $R_{pq} = a_{pq} - \sum_{q<\tau<p} g_{p\tau} b_{\tau q}$ is given by induction and $\tilde{U}$ is a suitable operator which exploits the symmetry of g_{pq}.

Lately, we have been trying to generalize the above results to *Schubert varieties with two conditions*. As the name suggests, we no longer fix a subspace, yet a flag $0 \neq F_1 \subset F_2 \subset \mathbb{C}^l$ and, consequently, two suitably integers $0 < i_1 < i_2$. Then, $\mathcal{S} = \{V \in \mathbb{G}_k(\mathbb{C}^l) : \dim(V \cap F_\alpha) \geq i_\alpha, \alpha = 1, 2\}$ is called a *Schubert variety with two conditions*. In this more general setting, there is still a resolution of singularities $\pi : \tilde{\mathcal{S}} \to \mathcal{S}$, where $\tilde{\mathcal{S}} = \{(Z_1, Z_2, V) \in \mathbb{G}_{i_1}(F_1) \times \mathbb{G}_{i_2}(F_2) \times \mathbb{G}_k(\mathbb{C}^l) : Z_1 \subseteq Z_2 \subseteq V\}$ and the Decomposition theorem gives an isomorphism analogous to (1). Again, we are able to describe each direct summand in this isomorphism by generalizing (2), despite the lack of some pieces of information which are available in the special case. As a consequence, we obtain the local description of the intersection cohomology complex of $\mathcal{S}$; that is, its restriction to the smooth locus of any of its strata, and a Poincaré polynomial identity analogous to (3). In this case, the polynomials corresponding to the ones we denoted by b_{pq} and g_{pq} are unknown, yet, from the discussion above, there is an iterative algorithm similar to (4), which can compute them all.

Keywords

Leray–Hirsch theorem, Derived category, Intersection cohomology, Decomposition theorem, Schubert varieties, Resolution of singularities

References

[1] A. A. Beilinson; J. Bernstein; P. Deligne, Faisceaux pervers. *Astérisque* **100**, 5–171 (1982).

[2] S. Billey; V. Lakshimbdai, *Singular loci of Schubert varieties*, Springer, New York, 2000.

[3] F. Cioffi; D. Franco; C. Sessa, Polynomial identities related to Special Schubert varieties. *AAECC*, doi: 10.1007/s00200-021-00496-6 (2021).

[4] M. A. de Cataldo; L. Migliorini, The Hodge theory of algebraic maps. *ASENS* **38**(5), 693–750 (2005).

[5] M. A. de Cataldo; L. Migliorini, The decomposition theorem, perverse sheaves and the topology of algebraic maps. *Bulletin of the American Mathematical Society* **46**(4), 535–633 (2009).

[6] V. Di Gennaro; D. Franco, Néron-Severi group of a general hypersurface. *Communications in Contemporary Mathematics* **19**(01), 1–15 (2017).

[7] V. Di Gennaro; D. Franco, On a Resolution of Singularities with Two Strata. *Results in Mathematics* **74**(3), 74–115 (2019).

[8] D. Franco, Explicit decomposition theorem for special Schubert varieties. *Forum Mathematicum* **32**(2), 447–470, (2020).

[9] S. I. Gelfand; Y. I. Manin, *Methods of Homological Algebra (2nd ed.).* Springer-Verlag Berlin, 2003

[10] L. Manivel, *Symmetric functions, Schubert polynomials and degeneracy loci.* American Mathematical Society, 2001.

[11] C. Voisin, *Hodge Theory and Complex Algebraic Geometry, I.* Cambridge University Press, 2002.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic Geometry from an algorithmic point of view”*

Hyperplane arrangements and k-Lefschetz properties

Michele Torielli[1]***, Elisa Palezzato***[2] [torielli@math.sci.hokudai.ac.jp]

[1] Department of Mathematics, GI-CoRE GSB, Hokkaido University, Sapporo, Japan
[2] Department of Mathematics, Hokkaido University, Sapporo, Japan

1 Lefschetz and k-Lefschetz properties

Let $\mathbb{K}$ be a field of characteristic 0 and $R = \bigoplus_{i\geq 0} R_i$ a graded ring over $\mathbb{K}$, where R_i are the homogeneous components of R with $\dim_{\mathbb{K}}(R_i) < \infty$. R is said to have the **weak Lefschetz property (WLP)**, if there exists an element $\ell \in R_1$ such that the multiplication map $\times\ell\colon R_i \to R_{i+1}$ is full-rank for every $i \geq 0$. In this case, ℓ is called a **weak Lefschetz element**. Similarly, R is said to have the **strong Lefschetz property (SLP)**, if there exists an element $\ell \in R_1$ such that the multiplication map $\times\ell^s\colon R_i \to R_{i+s}$ is full-rank for every $i \geq 0$ and $s \geq 1$. In this case, ℓ is called a **strong Lefschetz element**.
The notions of weak and strong k-Lefschetz properties were introduced in [4] as a generalization of the weak and strong Lefschetz properties. See also [3] and [5]. If we consider k a positive integer, then the graded ring R is said to have the ***k*-SLP** (respectively the ***k*-WLP**) if there exist elements $\ell_1, \dots, \ell_k \in R_1$ such that R has the SLP (respectively WLP) with Lefschetz element ℓ_1 and $R/\langle \ell_1, \dots, \ell_{i-1}\rangle$ has the SLP (respectively WLP) with Lefschetz element ℓ_i, for all $i = 2, \dots, k$. In this case we will say that $(R, \ell_1, \dots, \ell_k)$ has the k-SLP (respectively k-WLP).
The following result shows that we can reduce the study of the k-Lefschetz properties to the monomial case using $\mathrm{rgin}(I)$, the **generic initial ideal** with respect to the ordering $DegRevLex$ (see [1] for more details on rgin).

Theorem 1.1 (Theorem 3.6, [7])**.** *Let I be a homogeneous ideal of $S = \mathbb{K}[x_1, \dots, x_l]$ and $1 \leq k \leq l$. Then the following two conditions are equivalent*

1. *S/I has the k-SLP (respectively the k-WLP),*
2. *$(S/\mathrm{rgin}(I), x_l, \dots, x_{l-k+1})$ has the k-SLP (respectively the k-WLP).*

In the study of k-Lefschetz properties an important role is played by the so called almost revlex ideals, where a monomial ideal I of S is called an **almost revlex ideal**, if for any power-product t in the minimal generating set of I, every other power-product t' of S with $\deg(t') = \deg(t)$ and $t' >_{DegRevLex} t$ belongs to the ideal I.

Theorem 1.2 (Theorem 4.6, [7]). *Let I be an almost revlex ideal of S. Then $(S/I, x_l, \dots, x_1)$ has the l-SLP.*

Theorem 1.3 (Theorem 5.8, [8]). *Let I be a homogeneous ideal of $S = \mathbb{K}[x, y, z]$ such that S/I has the SLP. Then $\operatorname{rgin}(I)$ is an almost revlex ideal and it is uniquely determined by the Hilbert function of I.*

The following result relates the study of the non-Artinian case with the Artinian one

Theorem 1.4 (Theorem 5.4, Corollary 5.5, Theorem 5.6, [7]). *Let I be a homogeneous ideal of S and $1 \leq k \leq l$. Then the following facts are equivalent*

1. *the graded ring S/I has the k-SLP (respectively the k-WLP),*
2. *the graded Artinian ring $S/\hat{I}$ has the k-SLP (respectively the k-WLP), where $\hat{I} = I + \langle x_1, \dots, x_l\rangle^{\operatorname{reg}(I)+1}$.*

Moreover, I is an almost revlex ideal if and only if $\hat{I}$ is an almost revlex ideal.

2 Hyperplane arrangements and k-Lefschetz properties

A finite set of affine hyperplanes $\mathcal{A} = \{H_1, \dots, H_n\}$ in $\mathbb{K}^l$ is called a **hyperplane arrangement**. For each hyperplane H_i we fix a defining linear polynomial $\alpha_i \in S$ such that $H_i = \alpha_i^{-1}(0)$, and let $Q(\mathcal{A}) = \prod_{i=1}^n \alpha_i$. An arrangement $\mathcal{A}$ is called **central** if each H_i contains the origin of $\mathbb{K}^l$. In this case, each $\alpha_i \in S$ is a linear homogeneous polynomial, and hence $Q(\mathcal{A})$ is homogeneous of degree n. We denote by $\operatorname{Der}_{\mathbb{K}^l} = \{\sum_{i=1}^l f_i \partial_{x_i} \mid f_i \in S\}$ the S-module of **polynomial vector fields** on $\mathbb{K}^l$ (or S-derivations). We will say that a central arrangement $\mathcal{A}$ is **free** if and only if the **module of vector fields logarithmic tangent** to $\mathcal{A}$ (or logarithmic vector fields) $D(\mathcal{A}) = \{\delta \in \operatorname{Der}_{\mathbb{K}^l} \mid \delta(\alpha_i) \in \langle \alpha_i \rangle, \forall i\}$ is a free S-module. If we denote by $J(\mathcal{A})$ the **Jacobian ideal** of $\mathcal{A}$, we can connect it to the study of free arrangements (see also [6]).

Theorem 2.1 (Theorem 5.4, [2]). *Let $\mathcal{A} = \{H_1, \dots, H_n\}$ be a central arrangement in $\mathbb{K}^l$. Then $\mathcal{A}$ is free if and only if $\operatorname{rgin}(J(\mathcal{A}))$ coincides with S or it is minimally generated by*

$$x_1^{n-1},\ x_1^{n-2}x_2^{\lambda_1},\ \dots,\ x_2^{\lambda_{n-1}}$$

with $1 \leq \lambda_1 < \lambda_2 < \cdots < \lambda_{n-1}$ and $\lambda_{i+1} - \lambda_i = 1$ or 2.

Conjecture 2.2 (Conjecture 5.7, [2]). *Let $\mathcal{A}$ be a central arrangement in $\mathbb{K}^l$ and $d_0 = \min\{d \mid x_2^d \in \operatorname{rgin}(J(\mathcal{A}))\}$. If $\operatorname{rgin}(J(\mathcal{A}))$ has a minimal generator t that involves the third variable of S, then $\deg(t) \geq d_0$.*

The study of the Lefschetz properties has already been linked to the theory of arrangements, see for example [8]. The following results deepen this connection.

Proposition 2.3 (Lemma 8.1, [7])**.** *Let $\mathcal{A}$ be a central arrangement in $\mathbb{K}^2$. Then $S/J(\mathcal{A})$ has the 2-SLP.*

Putting together Theorem 8.2 of [7], and Theorem 8.5 and Proposition 8.10 of [8], we obtain the following result.

Theorem 2.4. *Let $\mathcal{A}$ be a free arrangement in $\mathbb{K}^l$. Then*

1. *$S/J(\mathcal{A})$ has the l-SLP,*
2. *$S/J(\mathcal{A})$ has an increasing Hilbert function,*
3. *$\operatorname{rgin}(J(\mathcal{A}))$ is an almost revlex ideal.*

Improving on the study of [7] and [8], we have the following result.

Theorem 2.5. *Let $\mathcal{A}$ be a central arrangement in $\mathbb{K}^3$. Then $S/J(\mathcal{A})$ has the 3-WLP and Conjecture 2.2 holds for $\mathcal{A}$.*

Remark 2.6. *It is not hard to construct examples of central arrangement in $\mathbb{K}^3$ such that $S/J(\mathcal{A})$ does not have the SLP and examples of central arrangement in $\mathbb{K}^l$, with $l \geq 4$, such that $S/J(\mathcal{A})$ does not have the WLP.*

Keywords
Lefschetz Properties, Almost Revlex Ideals, Hyperplane Arrangements

References

[1] A. M. Bigatti, E. Palezzato, and M. Torielli, Extremal behavior in sectional matrices. *Journal of Algebra and its Applications*, 18(3), (2019).
[2] A. M. Bigatti, E. Palezzato, and M. Torielli, New characterizations of freeness for hyperplane arrangements. *Journal of Algebraic Combinatorics*, 51(2), 297–315 (2020).
[3] T. Harima, T. Maeno, H. Morita, Y. Numata, A. Wachi, and J. Watanabe, *The Lefschetz properties*, volume 2080 of Lecture Notes in Mathematics. Springer, 2013.
[4] T. Harima and A. Wachi, Generic initial ideals, graded Betti numbers, and k-Lefschetz properties. *Communications in Algebra*, 37(11), 4012–4025 (2009).
[5] J.C. Migliore and U. Nagel, Survey article: a tour of the weak and strong Lefschetz properties. *Journal of Commutative Algebra*, 5(3), 329–358 (2013).
[6] E. Palezzato and M. Torielli, Free hyperplane arrangements over arbitrary fields. *Journal of Algebraic Combinatorics*, 52(2), 237–249 (2020).
[7] E. Palezzato and M. Torielli, k-Lefschetz properties, sectional matrices and hyperplane arrangements. *arXiv:2003.06294*.
[8] E. Palezzato and M. Torielli, Lefschetz properties and hyperplane arrangements. *Journal of Algebra*, 555, 289–304 (2020).

S2. Hybrid Symbolic-Numeric Computation

Organized by

Robert M. Corless, Mark Giesbrecht, George Labahn and Leili Rafiee Sevyeri

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Hybrid Symbolic-Numeric Computation"*

Approximation of functions of structured matrices

Paola Boito[1], ***Yuli Eidelman***[2], ***Luca Gemignani***[3] [paola.boito@unipi.it]

[1] Department of Mathematics, Università di Pisa, Pisa, Italy
[2] School of Mathematical Sciences, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel-Aviv University, Ramat-Aviv, Israel
[3] Department of Computer Science, University of Pisa, Pisa, Italy

Rational approximation is a widespread approach to the computation of matrix functions. In this talk we discuss a family of rational approximations to the reciprocal of a ϕ-function that plays a role in the solution of linear differential problems. Such approximations, introduced in [1], are especially well-suited to the computation of functions of rank-structured matrices. They can also be used to formulate bounds describing the off-diagonal decay properties of these matrix functions. Computational tests include comparisons to polynomial and Padé approximations, both in the scalar and matrix case.

Keywords
Matrix functions, Rational approximation, structured matrices

References

[1] P. BOITO, Y. EIDELMAN, L. GEMIGNANI, Computing the reciprocal of a ϕ-function by rational approximation, arXiv:1801.04573 [math.NA] (2021).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Hybrid Symbolic-Numeric Computation*

Symbolic-numeric computing for Bohemian matrices

Robert M. Corless[1] [rcorless@uwaterloo.ca]

[1] David R. Cheriton School of Computer Science, University of Waterloo

A Bohemian matrix family is a set of matrices each of whose entries comes from a fixed, usually finite integer, population. Questions about the eigenvalues of the entire family turn out to be interesting on several fronts, and numerical methods for computing the eigenvalues are valuable because they are efficient and stable in a backward error sense. However, to answer certain combinatorial questions, exact computation can be better, and even symbolic computation (especially of inverse eigenvalue problems) can be useful. In this talk we explore some examples and give a theorem about some rare but important errors in purely numerical computation. This is joint work with many people, including Aaron Asner and Mark Giesbrecht.

Keywords
Bohemian matrix, Eigenvalues of Bohemian matrices

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Hybrid Symbolic-Numeric Computation"*

Sparse Interpolation: from de Prony to Froissart and beyond

Annie Cuyt[1,2] [annie.cuyt@uantwerpen.be]

[1] Department of Computer Science, University of Antwerp, Antwerpen, Belgium
[2] College of Mathematics and Statistics, Shenzhen University, Shenzhen, China

In 1795 the French mathematician de Prony [6] published a method to fit a real-valued exponential model to some uniformly collected samples, making use of a linear recurrence connecting the data.

In the beginning of the 20-th century the famous Nyquist constraint [10] was formulated, which is the digital signal processing equivalent of stating that the argument of a complex exponential $\exp(\phi\Delta)$ with $\phi \in \mathbb{C}$ and $\Delta \in \mathbb{R}^+$ can only be retrieved uniquely under the condition that $|\Im(\phi)| < \pi/\Delta$.

Both methods are closely connected to sparse interpolation from computer algebra.

In the past two decades the Nyquist constraint was first broken when using randomly collected signal samples [7, 2] and later for use with uniformly collected samples [4]. Besides discussing how to avoid the Nyquist constraint, we also explain how to solve a number of remaining open problems in exponential analysis using sparse interpolation results.

We start from the most general problem statement. In the identification, from given values $f_k \in \mathbb{C}$, of the nonlinear parameters $\phi_1, \dots, \phi_n \in \mathbb{C}$, the linear coefficients $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ and of the sparsity $n \in \mathbb{N}$ in the fitting problem

$$\sum_{j=1}^{n} \alpha_j \exp(\phi_j k\Delta) = f_k, \qquad k = 0, \dots, 2n-1, \dots \quad f_k \in \mathbb{C}, \quad \Delta \in \mathbb{R}^+, \tag{1}$$

several cases are considered to be hard [4, 1]:

- When some of the ϕ_j cluster, the identification and separation of these clustered ϕ_j becomes numerically ill-conditioned. We show how the problem may be reconditioned.
- From noisy f_k samples, retrieval of the correct value of n is difficult, and more so in case of clustered ϕ_j. Here, decimation of the data offers a way to obtain a reliable estimate of n automatically.

- Such decimation allows to divide and conquer the inverse problem statement. The smaller subproblems are largely independent and can be solved in parallel, leading to an improved complexity and efficiency.
- At the same time, the sub-Nyquist Prony method proves to be robust with respect to outliers in the data. Making use of some approximation theory results [8, 9], we can also validate the computation of the ϕ_j and α_j.
- The Nyquist constraint effectively restricts the bandwidth of the $\Im(\phi_j)$. Therefore, avoiding the constraint offers so-called superresolution, or the possibility to unearth higher frequency components in the samples.

All of the above can be generalized in several ways, on the one hand to [5] the use of more functions besides the exponential, and on the other hand [3] to the solution of multidimensional inverse problems as in (1).

Keywords
sparse interpolation, exponential analysis, Nyquist, Padé, Prony, Froissart

References

[1] M. Briani, A. Cuyt, F. Knaepkens, and W.-s. Lee, VEXPA: Validated EXPonential Analysis through regular subsampling. *Signal Processing* **177**, 107722 (2020).
[2] E. J. Candès, J. Romberg, and T. Tao, Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. *IEEE Transactions on Information Theory* **52**(2), 489–509 (206).
[3] A. Cuyt and W.-s. Lee, Multivariate exponential analysis from the minimal number of samples. *Advances in Computational Mathematics* **44**(4), 987–1002 (2018).
[4] A. Cuyt and W.-s. Lee, How to get high resolution results from sparse and coarsely sampled data. *Applied and Computational Harmonic Analysis* **48**(3), 1066–1087 (2020).
[5] A. Cuyt and W.-s. Lee, Parametric spectral analysis: scale and shift. *ArXiv* e-print 2008.02125 [cs.NA], Universiteit Antwerpen (2020).
[6] R. de Prony, Essai expérimental et analytique sur les lois de la dilatabilité des fluides élastiques et sur celles de la force expansive de la vapeur de l'eau et de la vapeur de l'alkool, à différentes températures. *Journal de l'École Polytechnique* **1**(22), 24–76 (1795).
[7] D. L. Donoho, Compressed sensing. *IEEE Transactions on Information Theory* **52**(4), 1289–1306 (2006).
[8] J. Gilewicz and M. Pindor, Padé approximants and noise: a case of geometric series. *Journal of Computational and Applied Mathematics* **87**(2), 199–214 (1997).
[9] J. Gilewicz and M. Pindor, Padé approximants and noise: rational functions. *Journal of Computational and Applied Mathematics* **105**(1-2), 285–297 (1999).
[10] H. Nyquist, Certain topics in telegraph transmission theory. *Transactions of the American Institute of Electrical Engineers* **47**(2), 617–644 (1928).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Hybrid Symbolic-Numeric Computation"*

Sparse Interpolation: design sparse antenna arrays for estimating directions of arriving signals

Wen-shin Lee [wen-shin.lee@stir.ac.uk]

Division of Computing Science and Mathematics, University of Stirling, Scotland, UK

Estimating the directions of simultaneously arriving signals plays an important role in radar, remote sensing, radio frequency interference mitigation, wireless networks, machine perception of unmanned aerial vehicles or self-driving cars. In signal processing, antenna array systems have been designed to solve the problem of estimating the direction of arrival (DOA). A main constraint in designing regularly spaced antenna systems is the spatial Nyquist criterion, which requires the space between two sensors to be less than half of the signal wavelength. A disadvantage of densely spaced antenna elements is the effect of mutual coupling, normally reduced through costly extensive calibration of the system.

Using a regularly spaced antenna system for DOA estimation can be formulated as an exponential analysis problem, which can be tackled by the classical Prony method from approximation theory. Interestingly, the Ben-Or/Tiwari sparse interpolation algorithm in computer algebra is closely related to Prony's method. This connection has led to a major development in exponential analysis that can circumvent the Nyquist constraint [1], hence allow us to completely remove the dense Nyquist spacing requirement for DOA in antenna design [2].

Keywords
direction of arrival, exponential analysis, sparse interpolation

References

[1] A. Cuyt and W.-s. Lee, How to get high resolution results from sparse and coarsely sampled data. *Applied and Computational Harmonic Analysis* **48**(3), 1066–1087 (2020).

[2] F. Knaepkens, A. Cuyt, W.-s. Lee and D. I. L. de Villiers, Regular sparse array direction of arrival estimation in one dimension. *IEEE Transactions on Antennas and Propagation* **68**(5), 3997–4006 (2020).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Hybrid Symbolic-Numeric Computation”*

On the problem of the approximate parametrization of algebraic curves and surfaces and some applications

Sonia Pérez-Díaz[1,2] [sonia.perez@uah.es]

[1] Universidad de Alcalá, Dpto. de Física y Matemáticas, 28871-Alcalá de Henares, Madrid, Spain

[2] Partially supported by FEDER/Ministerio de Ciencia, Innovación y Universidades-Agencia Estatal de Investigación/MTM2017-88796-P (Symbolic Computation: new challenges in Algebra and Geometry together with its applications)

We deal with the problem of parametrizing approximately a perturbed rational curve/surface implicitly given. We present some of our algorithms ([1], [2], [4]) and we describe applications in this context ([3], [5], [6], [7]). More precisely, we focus on the approximate parametrization algorithms, and we show that the input and output curves/surfaces of the algorithm are close. Finally, we show how these results give the key to deal with some additional questions as the numerical proper reparametrization, the numerical polynomial reparametrization or detecting whether an input surface is ”almost´´ a ruled surface.

Keywords
Approximate parametrization, error analysis, ϵ–singularity, numerical reparametrization.

References

[1] S. PÉREZ-DÍAZ; J.R. SENDRA; J. SENDRA, Parametrizations of Approximate Algebraic Curves by Lines. *Theoretical Computer Science*, **volume**(315/2-3), 627-650. (2004).
[2] S. PÉREZ-DÍAZ; J.R. SENDRA; J. SENDRA, Parametrizations of Approximate Algebraic Surfaces by Lines. *Computer Aided Geometric Design*, **volume**(22/2), 147-181. (2005).
[3] S. PÉREZ-DÍAZ; J.R. SENDRA; J. SENDRA, Distance Bounds of ϵ-Points on Hypersurfaces. *Theoretical Computer Science*, **volume**(359, n. 1-3), 344-368. (2006).
[4] S. PÉREZ-DÍAZ; S.L. RUEDA; J.R. SENDRA; J. SENDRA, Approximate parametrization of plane algebraic curves by linear systems of curves. *Computer Aided Geometric Design*, **volume**(27), 212–231. (2010).
[5] S. PÉREZ-DÍAZ; L.Y. SHEN; Z. YANG, Numerical Proper Reparametrization of Space Curves and Surfaces. *Computer Aided-Design*, **volume**(116), 1-16. 102732. (2019).
[6] S. PÉREZ-DÍAZ; L.Y. SHEN, Numerical Polynomial Reparametrization of Rational Curves. *Computer Aided Geometric Design*, **volume**(71), 90-104. (2019).
[7] S. PÉREZ-DÍAZ; L.Y. SHEN, A Symbolic-Numeric Approach for Parametrizing Ruled Surfaces. *Journal of Systems Science and Complexity*, **volume**(33), 799–820. (2020).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Hybrid Symbolic-Numeric Computation"*

Linearizations of transfer function matrices

María C. Quintana[1], ***Javier Pérez***[2] [maria.quintanaponce@aalto.fi]

[1] Department of Mathematics and Systems Analysis, Aalto University, Aalto, Finland;
[2] Department of Mathematical Sciences, University of Montana, Montana, USA.

Given a rational matrix $R(\lambda)$, the Rational Eigenvalue Problem (REP) consists of finding scalars λ_0 (eigenvalues) such that there exist nonzero constant vectors x and y (eigenvectors) satisfying

$$R(\lambda_0)x = 0 \quad \text{and} \quad y^T R(\lambda_0) = 0,$$

under the regularity assumption det $R(\lambda) \not\equiv 0$. The numerical solution of REPs is recently getting a lot of attention from the numerical linear algebra community since REPs appear directly from applications or as approximations to arbitrary nonlinear eigenvalue problems. Rational matrices also appear in linear systems and control theory. Nowadays, a competitive method for solving REPs is linearization. Linearization transforms the REP into a generalized eigenvalue problem in such a way that the pole and zero information of the corresponding rational matrix is preserved. In this talk, we present a new family of local linearizations of rational matrices, by considering the definition of local linearizations in [1]. We use the fact that any rational matrix $R(\lambda)$ can be written as the transfer function matrix of a polynomial system matrix. That is, of the form $R(\lambda) = D(\lambda) + C(\lambda)A(\lambda)^{-1}B(\lambda)$, where $D(\lambda)$, $C(\lambda)$, $B(\lambda)$ and $A(\lambda)$ are polynomial matrices. Then, the new linearizations are constructed from linearizations of the polynomial matrices $D(\lambda)$ and $A(\lambda)$, where each of them can be represented in terms of any polynomial basis. We show by example how this theory can be used for solving scalar rational equations.

Keywords
rational matrix, transfer function matrix, polynomial system matrix, rational eigenvalue problem, local linearization

References

[1] F. M. Dopico, S. Marcaida, M. C. Quintana, P. Van Dooren, Local linearizations of rational matrices with application to rational approximations of nonlinear eigenvalue problems. *Linear Algebra Appl.* **604**, 441–475 (2020).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Hybrid Symbolic-Numeric Computation"*

Hybrid Symbolic-Numeric Algorithms for Approximate GCD

***Leili Rafiee Sevyeri*, Robert M. Corless** [lrafiees@uwaterloo.ca]

David R. Cheriton School of Computer Science, University of Waterloo, Canada

We introduce hybrid symbolic-numeric methods which solve the *approximate* `GCD` problem for polynomials presented in Bernstein and Lagrange bases.

We adapt Victor Y. Pan's root-based algorithm for finding approximate GCD to the case where the polynomials are expressed in Bernstein bases. We use the numerically stable companion pencil of Guðbjörn Jónsson to compute the roots, and the Hopcroft-Karp bipartite matching method to find the degree of the approximate GCD. We offer some refinements to improve the process.

We also introduce an algorithm with similar idea, which finds an approximate GCD for a pair of approximate polynomials given in a Lagrange basis. More precisely, we suppose that these polynomials are given by their approximate values at distinct known points. We first find each of their roots by using a Lagrange basis companion pencil for each polynomial. We introduce new clustering algorithms and use them to cluster the roots of each polynomial to identify multiple roots, and then *marry* the two polynomials using a *Maximum Weight Matching* algorithm, to find their GCD.

Keywords
Bernstein basis, Approximate GCD , Maximum matching, Root clustering, Lagrange basis, Maximum weight matching

References

[1] ROBERT M. CORLESS, AND LEILI RAFIEE SEVYERI, Approximate GCD in a Bernstein Basis. In *Maple in Mathematics Education and Research*, Jürgen Gerhard and Ilias Kotsireas (eds.), 77–91, Waterloo, 2020.
[2] LEILI RAFIEE SEVYERI AND ROBERT M. CORLESS, Approximate GCD in Lagrange bases. In *2020 22nd International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)*, 40-47, Timisoara, 2020.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Hybrid Symbolic-Numeric Computation"*

Multivariate Approximate GCD Computation Using Null Space of Subresultant Matrix within Polynomials: Non-singular Case

Masaru Sanuki[1] [sanuki@md.tsukuba.ac.jp]

[1] Faculty of Medicine, University of Tsukuba, Ibaraki 305-8575, Japan

In this talk, we discuss how to compute null space of subresultant matrix within polynomials, for multivariate approximate GCD computation with floating-point numbers. Our idea is used numerical computation (null space of numeric matrix) for univariate part and mathematical processing (lifting technique) for multivariate part in order to pursue accuracy and efficiency, such as [3]. Actually, the size of subresultant matrix is not big, it is the sum of degrees of given polynomials w.r.t. the main variable. (the size of generalized subresultant matrices within numeric will be huge [2, 4]). Show several tests.

keywords
multivariate approximate GCD, matrix computation within polynomials, null space

References

[1] R. Corless, P. Gianni, B. Trager and S. Watt, *The singular value decomposition for polynomial systems*, Proc. of ISSAC'95, ACM Press, 1995, 195–207.

[2] S. Gao, E. Kaltofen, J. P. May, Z. Yang and L. Zhi, *Approximate factorization of multivariate polynomials via differential equations*, Proc. of ISSAC'04, ACM Press, 2004, 167–174.

[3] M. Sanuki. *Computing multivariate approximate GCD based on Barnett's theorem*, Proc. of Symbolic-Numeric Computation 2009 (SNC 2009), 2009, 149–157.

[4] Z. Zeng and B. H. Dayton, *The approximate GCD of inexact polynomials part II: A multivariate algorithm*, Proc. of ISSAC'04, ACM Press, 2004, 320–327.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Hybrid Symbolic-Numeric Computation”*

The Nearest Function Represented by a Convex Combination of Given Functions with Constraints

Hiroshi Sekigawa[1] [sekigawa@rs.tus.ac.jp]

[1] Department of Applied Mathematics, Tokyo University of Science, Tokyo, Japan

Given functions f, f_1, $\dots$, f_n and constraints, we investigate a problem of finding the nearest function to f represented by a convex combination of f_i's and satisfying the constraints. Furthermore, using the results, we investigate complex dynamics of a rational function represented by a convex combination of Möbius transformations, whose combination coefficients have errors.

Keywords
Convex combination, Perturbation, Möbius transformation, Complex dynamics

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Hybrid Symbolic-Numeric Computation"*

Solving Irregular Triangular Systems: a Truly Local Approach

Chee Yap[1]***, R. Imbach and M. Pouget*** [yap@cs.nyu.edu]

[1] Department of Computer Science of Courant Institute of Mathematical Science, New York University.

Root isolation, and more generally root clustering, of a univariate polynomial is a fundamental computational problem. In the last 5 years, we have seen the development of novel asymptotically "near-optimal" algorithms that are both implementable and practical.

To extend these advances to the multivariable setting, we consider the problem of clustering the zeros of a 0-dimensional triangular polynomial system,

$$f_1(x_1) = \cdots = f_n(x_1, \ldots, x_n) = 0.$$

All current algorithms require the system to satisfy some conditions of "regularity". In this talk, we introduce a new technique that avoids any such condition. Our algorithm operates in a very general setting where the coefficients of f_i's are oracle complex numbers.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Hybrid Symbolic-Numeric Computation”*

Verifying the Positivity of a Function over a Finite Set

***Lihong Zhi*, Jianting Yang, Ke Ye** [lzhi@mmrc.iss.ac.cn]

KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China

Given a finite set $S = \{s_0, s_1, s_2, ..., s_{N-1}\}$, we aim to verify that a map f from S to $\mathbb{R}$ is nonnegative, i.e. $f(s) \geq 0$ for each $s \in S$. We propose the following method:

(1) Choose a finite abelian group $G = \{g_0, g_1, g_2, ..., g_{N-1}\}$, define a bijection $\phi : G \mapsto S$, $s_i = \phi(g_i)$ for $0 \leq i \leq N - 1$;

(2) We verify that $f \circ \phi$ is a nonnegative function on G via computing its sparse sum-of-squares representation on abelian group G.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Hybrid Symbolic-Numeric Computation”*

Hermite Interpolation With Error Correction

Erich L. Kaltofen[1,2] [kaltofen ät ncsu döt edu]
[1] Department of Mathematics, NCSU, Raleigh, NC, USA
[2] Department of Computer Science, Duke University, Durham, NC, USA

Univariate polynomial interpolation with error correction is the methodology of the 1960 Reed-Solomon algebraic error correction code. Univariate polynomial Hermite interpolation with error correction, which fits values and values of derivatives, is the 1997 methodology of Rosenbloom-Tsfasman multiplicity error correction code. The Welch-Berlekamp decoding algorithm applies to both problems, and can be formulated as a numerically stable linear system. At ISSAC 2021 [1], Kaltofen, Pernet and Z.-H. Yang show that in the presence of a large error rate the multiplicity code is sub-optimal for fields of characteristic zero, that is, uses more values than are necessary for a unique interpolant. The interpolation algorithm at ISSAC 2021 does not use the Welch-Berlekamp error locator polynomial with multiplicities, and instead iterates the Reed-Solomon decoder. In my talk, I will investigate the numerical stability of our new Hermite interpolation algorithm with error correction.

Keywords
Hermite interpolation, Multiplicity error correction code, Reed-Solomon error correction code, high error capacity

[1] ERICH L. KALTOFEN; CLÉMENT PERNET; ZHI-HONG YANG, Hermite Interpolation With Error Correction: Fields of Zero or Large Characteristic and Large Error Rate. In *Proc. ISSAC 2021*, Marc Mezzarobba (eds.), ACM, New York, NY, 2021

S3. Computational Differential and Difference Algebra and its Applications

Organized by

Roberto La Scala, Alexander Levin and Daniel Robertz

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Computational Differential and Difference Algebra and its Applications"*

Mahler residues and telescopers for rational functions

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

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

We develop a notion of Mahler discrete residues for rational functions, with the desired property that a given rational function $f(x)$ is of the form $g(x^p) - g(x)$ for some rational function $g(x)$ (where p is an integer ≥ 2) if and only if all of its Mahler discrete residues vanish. We also show how to apply the technology of Mahler discrete residues to creative telescoping problems. This work extends to the Mahler case the earlier analogous notions, properties, and applications of discrete residues (in the shift case) and q-discrete residues (in the q-difference case) developed by Chen and Singer.

Keywords
Mahler summability, Mahler residues, telescoping problems

References

[1] C. ARRECHE; Y. ZHANG, Computing Differential Galois Groups of Second-Order Linear q-Difference Equations, *Advances in Applied Mathematics* (Accepted, 2021).

[2] S. CHEN; M.F. SINGER, Residues and Telescopers for Bivariate Rational Functions. *Advances in Applied Mathematics* **49**, 111–133 (2012).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Computational Differential and Difference Algebra and its Applications”*

Simplicity criteria for rings of differential operators in arbitrary characteristic

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

Two simplicity criteria are given for the algebra of differential operators $\mathcal{D}(R)$ on a commutative algebra R. One is for the algebra R of essentially finite type over a perfect field of arbitrary characteristic and another one for an arbitrary algebra R, [1]. This gives an answer to an old question of finding a simplicity criterion for algebras of differential operators.

Keywords
the ring of differential operators, simplicity criterion, normalization, Morita equivalence.

References

[1] V. V. Bavula, Simplicity criteria for rings of differential operators. *Glasgow Math. J.*, to appear (2021), arXiv:1912.07379.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Computational Differential and Difference Algebra and its Applications”*

Algebraic independance between special functions

***Boris Adamczewski*[1], *Thomas Dreyfus*[2], *Charlotte Hardouin*[3], *Michael Wibmer*[4]** [dreyfus@math.unistra.fr]

[1] CNRS, Université Lyon, France
[2] CNRS, Université Strasbourg, France
[3] Université Toulouse, France,
[4] Graz University, Austria

Let us consider a field equipped with two commuting automorphisms σ, ϕ. In this talk, we explain that for suitable choice of automorphisms, that a solution of a linear σ equation is algebraically independent of any solution of a ϕ-equation, unless, one of the the function is rational. As a consequence we obtain the proof of a conjecture by Van der Poorten of the algebraic independence of non rational p and q-Mahler function when p and q are multiplicatively independent.

Keywords
Difference field, Galois theory

References

[1] BORIS ADAMCZEWSKI, THOMAS DREYFUS, CHARLOTTE HARDOUIN, MICHAEL WIBMER, *Algebraic independence and linear difference equations*. To appear in Journal of the EMS.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Computational Differential and Difference Algebra and its Applications"*

An algebraic formulation of integral equations

Li Guo[1], ***Richard Gustavson***[2], ***Yunnan Li***[3] [liguo@rutgers.edu]

[1]Department of Mathematics and Computer Science, Rutgers University, Newark, NJ 07102, United States
[2] Department of Mathematics, Manhattan College, Riverdale, NY 10471, United States
[3] School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China

As the integral counterpart of differential equations, integral equations have a long history of study which has led to functional analysis and other developments.

In the algebraic context, differential equations are uniformly interpreted as elements of differential polynomial algebras. Such an interpretation for integral equations should come from a suitable notion of integral polynomial algebras, as the universal objects of integral algebras. Some special cases have be given by Rota-Baxter algebras and their generalizations.

We give a notion of integral algebras in the context of operated algebras [1] and their relative analogy, and provide a general formulation of integral equations from concrete constructions of free integral algebras by means of bracketed words and rooted trees with vertex and edge decorations. This also gives another viewpoint for differential equations and differential polynomial algebras. This talk is based on [2].

Keywords
Integral equation, Integral algebra, Operated algebra

References

[1] L. GUO, Operated semigroups, Motzkin paths and rooted trees. *J. Algebraic Combin.* **29**, 35–62 (2009).
[2] L. GUO; R. GUSTAVSON; Y. LI, *An algebraic study of Volterra integral equations and their operator linearity*. arXiv:2008.06756. (2020)

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Computational Differential and Difference Algebra and its Applications"*

Operator Linearity of Volterra Integral Equations

Li Guo[1], ***Richard Gustavson***[2], ***Yunnan Li***[3] [rgustavson01@manhattan.edu]

[1] Department of Mathematics and Computer Science, Rutgers University, Newark, NJ, USA
[2] Department of Mathematics, Manhattan College, Riverdale, NY, USA
[3] Department of Mathematics and Information Science, Guangzhou University, Guangzhou, China

A Volterra integral equation is an integral equation in which all integral operators are of the form

$$P(f)(x) := \int_a^x K(x,t)f(t)\,dt.$$

When the kernel $K(x,t)$ is simply 1, this Volterra integral operator reduces to the Rota-Baxter operator of weight zero. The algebraic structure of the space of such integral operators $\int_a^x f(t)\,dt$ using shuffle products was studied from this perspective and closely resembles the work of K.-T. Chen on iterated integrals [1], [2]. Since most applications of integral equations involve a nontrivial kernel, it is important to generalize these algebraic results. Specifically, a fundamental question is when an arbitrary integral equation can be expressed solely using iterated integrals.

In this talk we will focus on Volterra integral equations containing separable kernels of the form $K(x,t) = k(x)h(t)$. Under certain conditions on the kernel, these Volterra operators satisfy a twisted Rota-Baxter identity

$$P(f)P(g) = \tau P\left(\tau^{-1}P(f)g\right) + \tau P\left(\tau^{-1}fP(g)\right)$$

with twist $\tau = \frac{k(x)}{k(a)}$. This is a generalization of the integration-by-parts identity which appears in standard Rota-Baxter algebras, and can be extended to a matching twisted Rota-Baxter identity when multiple separable kernels are involved. We use the matching twisted Rota-Baxter algebra structure of separable Volterra operators to show that every Volterra integral equation involving separable kernels is equivalent to one that is operator linear, that is, does not involve any products of integrals [3].

Keywords
Volterra integral equation, Rota-Baxter algebra, iterated integral

References

[1] L. GUO, *An Introduction to Rota-Baxter Algebras*. International Press and Higher Education Press, Somerville, MA, USA and Beijing, China, 2012.

[2] K.-T. CHEN, Iterated path integrals. *Bull. Amer. Math. Soc.* **83**, 831–879 (1977).
[3] L. GUO; R. GUSTAVSON; Y. LI, An algebraic study of Volterra integral equations and their operator linearity. (2020). `https://arxiv.org/abs/2008.06756`.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Computational Differential and Difference Algebra and its Applications”*

Ciphers and Difference Algebra

Roberto La Scala [roberto.lascala@uniba.it]

Dipartimento di Matematica, Universita degli studi di Bari, Italy

Many stream or block ciphers of application interest such as Trivium, Bluetooth’s E0, Keeloq, etc can be modeled as systems of explicit ordinary difference equations over finite fields. Such systems indeed determine the evolution over discrete time of the internal state of these ciphers which is simply a vector with entries in a finite field. The use of the formal theory of algebraic difference equations, that is, Difference Algebra allows the study of some fundamental properties of difference ciphers, such as their invertibility and periodicity. This study implies the precise definition of algebraic attacks for the purpose of assessing cipher’s security. Such modeling and the corresponding cryptanalysis allows hence the development of new cryptosystems.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Computational Differential and Difference Algebra and its Applications”*

A New Type of Difference Dimension Polynomials

Alexander Levin [levin@cua.edu]

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

Let K be a difference field of characteristic zero with a basic set of (mutually commuting) endomorphisms $\sigma = \{\alpha_1, \dots, \alpha_m\}$, let T be the free commutative semigroup generated by σ, and for every $r, s \in \mathbb{N}$ with $s \leq r$, let $T(r, s) = \{\tau = \alpha_1^{k_1} \dots \alpha_m^{k_m} \in T \,|\, s \leq \operatorname{ord} \tau = \sum_{i=1}^{m} k_i \leq r\}$.
Let $R = K\{y_1, \dots, y_n\}$ be the algebra of difference (σ-) polynomials in σ-indeterminates $y_1, \dots, y_n$ and let TY denote the set of all *terms* in R, that is, the set of all elements of the form τy_i ($\tau \in T$, $1 \leq i \leq n$). If $u = \tau y_i$, we set $\operatorname{ord} u = \operatorname{ord} \tau$. In what follows, we assume that the following orderly ranking $\leq$ of the set of σ-indeterminates $y_1, \dots, y_n$ is fixed: if $u_1 = \alpha_1^{k_1} \dots \alpha_m^{k_m} y_i, u_2 = \alpha_1^{l_1} \dots \alpha_m^{l_m} y_j \in TY$, then $u_1 \leq u_2$ if and only if

$$(\operatorname{ord} u_1, k_1, \dots, k_m, i) \leq_{lex} (\operatorname{ord} u_2, l_1, \dots, l_m, j)$$

($\leq_{lex}$ denotes the lexicographic order on $\mathbb{N}^{m+2}$). In this case we set

$$\mu(u_2, u_1) = (\operatorname{ord} u_2 - \operatorname{ord} u_1, l_1 - k_1, \dots, l_m - k_m, j - i) \in \mathbb{N} \times \mathbb{Z}^{m+1}.$$

If $f \in K\{y_1, \dots, y_n\}$, then the greatest (with respect to the ranking $\leq$) term that appears in f is called the *leader* of f; it is denoted by u_f. If $u = u_f$ and $d = \deg_u f$, then the σ^*-polynomial f can be written as $f = I_d u^d + I_{d-1} u^{d-1} + \dots + I_0$ where $I_k (0 \leq k \leq d)$ do not contain u. The σ^*-polynomial I_d is called the *initial* of f; it is denoted by I_f. The lowest term in f is called the *coleader* of f and is denoted by v_f.
If $f \in R$, $u_f = \alpha_1^{k_1} \dots \alpha_m^{k_m} y_i$ and $v_f = \alpha_1^{l_1} \dots \alpha_m^{l_m} y_j$, then the nonnegative integer $\operatorname{Eord}(f) = \operatorname{ord} u_f - \operatorname{ord} v_f$ is called the **effective order** of f. The $(m+2)$-tuple $\mu(u_f, v_f) \in \mathbb{Z}^{m+2}$ is said to be the **full effective order** of f; it is denoted by $\mathcal{E}ord(f)$. In accordance with the above conventions, if $f, g \in R$, then $\mathcal{E}ord(f) \leq \mathcal{E}ord(g)$ means the $\mu(u_f, v_f)$ is less than or equal to $\mu(u_g, v_g)$ with respect to the lexicographic order on $\mathbb{Z}^{m+2}$. Of course, in this case $\operatorname{Eord}(f) \leq \operatorname{Eord}(g)$.
Let $f, g \in R$. We say that f is **E-reduced** with respect to g if f does not contain any $(\tau u_g)^e$ ($\tau \in T$) such that $e \geq d = \deg_{u_g} g$ and $\tau v_g \geq v_f$. Note that if $\mathcal{E}ord(f) < \mathcal{E}ord(g)$, then f is E-reduced with respect to g.
A set $\mathcal{A} \subseteq K\{y_1, \dots, y_n\}$ is said to be **E-autoreduced** if either it is empty or $\mathcal{A} \bigcap K = \emptyset$ and every element of $\mathcal{A}$ is E-reduced with respect to all other elements of $\mathcal{A}$. We show that every E-autoreduced set is finite.

If $f, g \in R$, we say that f has lower rank than g and write $\mathrm{rk}(f) < \mathrm{rk}(g)$ if either $\mathcal{E}ord(f) < \mathcal{E}ord(g)$, or $\mathcal{E}ord(f) = \mathcal{E}ord(g)$ and $u_f < u_g$, or $\mathcal{E}ord(f) = \mathcal{E}ord(g)$, $u_f = u_g = u$ and $\deg_u f < \deg_u g$. If $\mathrm{rk}(f) \not< \mathrm{rk}(g)$ and $\mathrm{rk}(g) \not< \mathrm{rk}(f)$, we say that f and g are of the same rank and write $\mathrm{rk}(f) = \mathrm{rk}(g)$.
If $\mathcal{A} = \{f_1, \dots, f_p\}$ and $\mathcal{B} = \{g_1, \dots, g_q\}$ are two E-autoreduced sets in R, we say that $\mathcal{A}$ is of lower rank than $\mathcal{B}$ and write $\mathrm{rk}(\mathcal{A}) < \mathrm{rk}(\mathcal{B})$ if either there exists $k \le \max\{p, q\}$ such that $\mathrm{rk}(f_i) = \mathrm{rk}(g_i)$ for $i < k$ and $\mathrm{rk}(f_k) < \mathrm{rk}(g_k)$, or $p > q$ and $\mathrm{rk}(f_i) = \mathrm{rk}(g_i)$ for $i = 1, \dots, q$.
We prove that every set of E-autoreduced sets in R contains an E-autoreduced set of lowest rank. If $\mathcal{A}$ is an E-autoreduced set of lowest rank among all E-autoreduced subsets of a difference ideal P of R, then $\mathcal{A}$ is said to be an E**-characteristic set** of P. The following theorem is the main result of the presentation.

Theorem. With the above notation, let $L = K\langle \eta_1, \dots, \eta_n \rangle$ be a difference field extension of K, let P be the defining difference ideal of the n-tuple $\eta = (\eta_1, \dots, \eta_n)$ in R, and let $\mathcal{A} = \{f_1, \dots, f_p\}$ be an E-characteristic set of P. Let $s_0 = \max\{\mathrm{Eord}(f_i) \,|\, 1 \le i \le p\}$. Then there exist a polynomial $\phi(t_1, t_2)$ in two variables with rational coefficients and $r_0 \in \mathbb{N}$ such that for all $r, s \in \mathbb{N}$ such that $r \ge r_0$ and $s_0 \le s \le r$, one has $\phi(r, s) = \mathrm{tr.deg}_K K\left(\bigcup_{i=1}^{n} T(r, s)\eta_i\right)$.

This result generalizes the well-known theorem on difference dimension polynomial (see [1]) and gives a more precise interpretation of the difference version of the concept of the Einstein's strength of a system of algebraic difference equations described in [2, Section 7.7].

Keywords
Effective order, E-autoreduced set, Dimension polynomial

References

[1] A. LEVIN, Characteristic polynomials of filtered difference modules and of difference field extensions. *Russian Math. Surveys* **33**(3), 165–166 (1978).
[2] A. LEVIN, *Difference Algebra.* Springer, New York,, 2008.

A division algorithm for Poisson algebras of graded Lie algebras

Omar Leon Sanchez[1] [omar.sanchez@manchester.ac.uk]

[1] Department of Mathematics, University of Manchester, UK

I will present a division algorithm for symmetric algebras, endowed with their natural Poisson structure, of graded Lie algebras. The algorithm, and the notions around it, is inspired by the division algorithm for differential polynomial rings and the notions of autoreducedness and characteristic sets. When the Lie algebra satisfies a suitable combinatorial condition (related to Dickson's lemma), this division algorithm yields a Poisson basis theorem on the symmetric algebra. I will point out that the combinatorial condition is satisfied by all graded simple Lie algebras of polynomial growth. This is joint work with Susan Sierra [1].

Keywords
graded Lie algebra, symmetric algebra, Poisson algebra

References

[1] O. LEON SANCHEZ AND S. SIERRA, *A Poisson basis theorem for symmetric algebras of infinite dimensional Lie algebras*. arXiv:2008.02845.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Computational Differential and Difference Algebra and its Applications”*

Weakly nonlocal Poisson brackets: algorithms and symbolic computation

Raffaele Vitolo [raffaele.vitolo@unisalento.it]

Department of Mathematics and Physics *E. De Giorgi*, Universita del Salento, Lecce, Italy

Weakly nonlocal Poisson brackets are an important subject in the Hamiltonian theory of partial differential equations. Examples of well-known integrable PDEs that admit weakly nonlocal Poisson brackets are the Korteweg-de Vries equation, the Camassa-Holm equation, the Krichever-Novikov equation, the nonlinear Schroedinger equation. Weakly nonlocal Poisson brackets are defined by a special class of linear integro-differential operators. In this talk we will illustrate new software packages in Maple, Reduce, Mathematica that aim at calculating the Jacobi property for weakly nonlocal Poisson brackets. A key feature of our approach is the identification of a canonical form that makes the calculation possible.

This is joint work with M. Casati, P. Lorenzoni, D. Valeri.
Preprint available at https://arxiv.org/abs/2101.06467, submitted to Computer Physics Communications.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Computational Differential and Difference Algebra and its Applications"*

On the computation of the dimension of systems of algebraic difference equations

Michael Wibmer[1] [wibmer@math.tugraz.at]

[1] Institute of Analyis and Number Theory, Graz University of Technology, Graz, Austria

Let k be a difference field and let $k\{y\} = k\{y_1, \ldots, y_n\}$ be the ring of difference polynomials over k in the difference variables $y_1, \ldots, y_n$. The *difference dimension* of a system $F \subseteq k\{y\}$ of algebraic difference equations over k can be defined as

$$\sigma\text{-}\dim(F) = \lim_{i\to\infty} \frac{d_i}{i+1},$$

where d_i is the Krull-dimension of $k\{y\}[i]/([F] \cap k\{y\}[i])$,

$$k\{y\}[i] = k[y_1, \ldots, y_n, \ldots, \sigma^i(y_1), \ldots, \sigma^i(y_n)]$$

is a polynomial ring in $n(i+1)$ variables over k and $[F] \subseteq k\{y\}$ is the difference ideal generated by F. See [1].

In case $[F]$ is a reflexive prime difference ideal, $\sigma\text{-}\dim(F)$ is the difference transcendence degree of the field of fractions of $k\{y\}/[F]$ over k. In particular, in this case, $\sigma\text{-}\dim(F)$ is an integer. In general, $\sigma\text{-}\dim(F)$ need not be an integer. For example, $\sigma\text{-}\dim(y_1\sigma(y_1)) = \frac{1}{2}$.

In this talk we will discuss some properties of the difference dimension and the challenges associated with computing the difference dimension.

Keywords
Difference dimension, systems of algebraic difference equations

References

[1] M. WIBMER, *On the dimension of systems of algebraic difference equations*. *Adv. in Appl. Math.* **123**, (2021).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Computational Differential and Difference Algebra and its Applications"*

Construction of free differential algebras by extending Gröbner-Shirshov bases

Li Guo[1], ***Yunnan Li***[2] [ynli@gzhu.edu.cn]

[1] Department of Mathematics and Computer Science, Rutgers University, Newark, NJ, USA
[2] School of Mathematics and Information Science, Guangzhou University, Guangzhou, China

As a fundamental notion, the free differential algebra on a set is concretely constructed as the polynomial algebra on the differential variables. Such a construction is not known for the more general notion of the free differential algebra on an algebra, from the left adjoint functor of the forgetful functor from differential algebras to algebras, instead of sets. The recent study of Poinsot expressed such free differential algebras as quotients.

We consider the more general case when the differential operator has a weight and when the algebra is not necessarily commutative [1]. We show that generator-relation properties of a base algebra can be extended to the free differential algebra on this algebra. More precisely, the Gröbner-Shirshov basis property of the base algebra can be extended to provide a Poincaré-Birkhoff-Witt type basis for these more general free differential algebras. Examples are given as illustrations. This talk is based on [2].

Keywords
Gröbner-Shirshov basis, differential algebra, free differential algebra

References

[1] L. Guo; W. Keigher, On differential Rota-Baxter algebras. *J. Pure Appl. Algebra* **212**, 522–540 (2008).
[2] L. Guo; Y. Li, Construction of free differential algebras by extending Gröbner-Shirshov bases. *J. Symbolic Comput.* **107**, 167–189 (2021).

S4. Effective Ideal Theory in Commutative and non-Commutative Rings and its Applications

Organized by

Michela Ceria, André Leroy and Teo Mora

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Effective Ideal Theory in Commutative and non-Commutative Rings and its Applications*

About Skew Reed-Solomon Codes

Delphine Boucher[1] [delphine.boucher@univ-rennes1.fr]

[1] IRMAR (UMR 6625), Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes Cedex

Skew Reed-Solomon codes over a division ring A are a generalization of Reed-Solomon codes ([2], [3]). They are obtained by evaluating skew polynomials at some particular points. These codes are optimal for the skew polynomial metric ([2], [4]) which is a generalization of the Hamming metric.

The ring R of skew polynomials over A is the set of polynomials $\sum a_i X^i$ over A endowed with the classical additive law and the multiplicative law given by : $\forall a \in A, X \cdot a = \theta(a)X + \delta(a)$ where θ is an endomorphism of A and δ is a derivation on A. This ring is Euclidean on the right: Euclidean division on the right, least common left multiples (lclm) and greatest common right divisors (gcrd) are well defined. For f in R and a in A the evaluation of f on a is defined as the remainder in the right division of f by $X - a$ (see [1]). When θ is the identity and δ is the zero derivation, the skew polynomial ring R is the classical ring, the skew evaluation is the classical evaluation, skew Reed-Solomon codes are classical Reed-Solomon codes and the skew polynomial metric is the Hamming metric.

This talk aims at presenting the family of skew Reed Solomon codes and the skew polynomial metric by using a simple formalism (mainly based on gcrd and lclm). This interpretation enables first to make the bridge with the classical Reed-Solomon codes and the Hamming metric in a simple way and secondly to design decoding algorithms which generalize the classical decoding algorithms for Reed-Solomon codes.

Keywords
skew polynomial ring, coding theory

References

[1] T. Y. LAM; A. LEROY, Vandermonde and Wronskian matrices over division rings. *Bull. Soc. Math. Belg. Sér. A* 40 (2), 281–286 (1987).
[2] U. MARTÍNEZ-PEÑAS, Skew and linearized Reed-Solomon codes and maximum sum rank distance codes over any division ring. *J. Algebra* 504, 587–612 (2018).
[3] D. BOUCHER; F. ULMER, Linear codes using skew polynomials with automorphisms and derivations. *Des. Codes Cryptogr.* 70 (3), 405–431 (2014).
[4] D. BOUCHER, An algorithm for decoding skew Reed-Solomon codes with respect to the skew metric. *Des. Codes Cryptogr.* 88 (9), 1991–2005 (2020).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Effective ideal theory in commutative and non commutative rings and its applications"*

The complexity of Weil descent polynomial systems

Alessio Caminata[1]***, Michela Ceria***[2]***, Elisa Gorla***[3] [caminata@dima.unige.it]

[1] Dipartimento di Matematica, Università degli Studi di Genova, Genova, Italy
[2] Department of Mechanics, Mathematics and Management, Politecnico di Bari, Bari, Italy
[3] Institut de Mathématiques, Université de Neuchâtel, Neuchâtel, Switzerland

Estimating the complexity of solving multivariate polynomial systems is relevant within Public-Key Cryptography and Coding Theory. We have two main classes of algorithms for computing Gröbner bases: Buchberger's Algorithm and linear algebra based algorithms, which transform the problem of computing a Gröbner basis into one or more instances of Gaussian elimination. Examples of linear algebra based algorithms are: F4, F5, the XL Algorithm, and MutantXL. Linear algebra based algorithms are often faster in practice and have contributed to breaking many cryptographic challenges. Some of these algorithms perform Gaussian elimination on the so-called Macaulay matrix M_d for increasing values of a parameter d. This parameter d, together with the number of polynomials in the system and the number of variables, determines the size of the corresponding matrix. The complexity of the algorithm is dominated by Gaussian elimination on the largest Macaulay matrix M_d encountered during this computation. The corresponding d is called **solving degree** of the system.

The definition of solving degree is algorithmic in its nature: If we would like to compute the solving degree of a polynomial system $\mathcal{F}$ we can run one of the above algorithms until the largest Macaulay matrix, and thus the solving degree, is found. However, for practical applications such as estimating the security of a cryptosystem, we would like to be able to find the solving degree without solving the system. In particular, in this talk we will be concerned with the following situation.

Let $\mathbb{F}_q$ be a finite field of cardinality q and let n be a positive integer. Let $\mathcal{F} \subseteq \mathbb{F}_{q^n}[x_1, \dots, x_m]$ be a polynomial system of inhomogeneous polynomials. We can associate to the system $\mathcal{F}$ another polynomial system $\mathrm{Weil}(\mathcal{F})$ over $\mathbb{F}_q$ called **Weil descent system** of $\mathcal{F}$. This is the system obtained by considering the Weil restriction of the polynomials of $\mathcal{F}$ to $\mathbb{F}_q$. Weil descent systems arise naturally in Public-Key Cryptography. For example, HFE systems are of this form, and the systems of the relation-collection phase of the index calculus algorithm for solving the DLP on an elliptic curve are coming from Weil restriction too. Using results from [1], we are able to prove that if $\mathcal{F}$ contains the field equations of $\mathbb{F}_{q^n}$ then

$$\mathrm{sd}\left(\mathrm{Weil}(\mathcal{F})\right) \leq n \cdot \mathrm{reg}(\mathcal{F}^h) - n + 1.$$

Here, sd is the solving degree with respect to a degree reverse lexicographic term order and $\mathrm{reg}(\mathcal{F}^h)$ denotes the Castelnuovo–Mumford regularity of the homogeneous ideal $(\mathcal{F}^h)$ generated by the homogenization of the polynomials of $\mathcal{F}$. In this talk, we will examine and motivate the previous upper bound on the solving degree of Weil descent systems. If time permits, we will discuss also some possible generalizations and applications.

Keywords
solving degree, Gröbner basis, Weil restriction

References

[1] A. CAMINATA, E. GORLA, Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra. In *Arithmetic of Finite Fields, 8th International Workshop*, J.C. Bajard and A. Topuzoglu Eds, Lecture Notes in Computer Science, vol. 12542, pp. 3–36, Springer, 2021.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Effective Ideal Theory in Commutative and non-Commutative Rings and its Applications”*

The use of Ideals in Algebraic Coding Theory

Steven Dougherty[1] [prof.steven.dougherty@gmail.com]

[1] Department of Mathematics, University of Scranton, Scranton Pennsylvania, USA.

Algebraic coding theory arose as an application to ensure effective communication over an electronic channel. Since then the field has developed into a branch of pure mathematics where the fundamental question is to find codes as subsets of A^n where A is an alphabet that satisfy a given condition. Classically, this condition was to have the largest minimum Hamming distance possible, but other such conditions have become important especially when studying codes over rings. For example, one may wish to find codes whose minimum distance with respect to other metrics is maximized, codes that are held invariant by the action of a certain group, or codes that are equal to their orthogonal. This type of coding theory is described in the text [1].

In this talk, we shall explain the use of ideals and the classification of ideals in algebraic coding theory over finite Frobenius rings. Specifically, we show how codes can be viewed as ideals in various rings and we give some paths for further research in this area. We shall discuss various families of codes where the study of ideals is central.

Keywords
Codes, Frobenius rings.

References

[1] STEVEN T. DOUGHERTY , *Algebraic Coding Theory over Finite Commutative Rings*. SpringerBriefs in Mathematics, Springer (ISBN 978-3-319-59805-5/pbk; 978-3-319-59806-2/ebook). x, 103 p. (2017).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Effective ideal theory in commutative and non commutative rings and its applications”*

The Maple library `SPBWE.lib` for working computationally with skew PBW extensions

William Fajardo [wafajardoc@unal.edu.co]

Departamento de Matemáticas, Universidad Nacional de Colombia, Bogotá, Colombia

In this talk we will present the `SPBWE.lib` library developed in Maple that allows to use the skew PBW extensions computationally. More exactly, the objects of interest to us are the *skew Poincaré-Birkhoff-Witt extensions* (skew PBW extensions for short) defined by Gallego and Lezama [10]. These extensions were introduced with the aim of generalizing the PBW extensions defined by Bell and Goodearl [3], the skew polynomial rings or Ore extensions of injective type introduced by Ore [19] and another noncommutative rings appearing in several contexts such as quantum groups, theory of differential operators, noncommutative algebraic geometry and noncommutative differential geometry. We remark that the importance of skew PBW extensions is that the coefficients do not necessarily commute with the variables, and these coefficients are not necessarily elements of fields, so these objects are different in these two aspects with respect to G-algebras. Ring and homological properties of skew PBW extensions have been studied by some authors, see Artamonov [2], Hamidizadeh et al., [12], Hashemi et al., [13], [14], Lezama et al., [1], [16], [18], Tumwesigye et al., [21], Zambrano [22] and the authors [4], [6] and [20]. In fact, a book has recently been published containing research results on ring theory, homological and computational properties of these extensions, see Fajardo et al., [5]. Precisely, since some of the homological properties of the skew PBW extensions are obtained using the notion of Gröbner basis (e.g., Fajardo [7], Gallego [8], [11] and Lezama et al., [10], [15], [17]). The implementation of the library allows to make effective some homological applications with skew PBW extensions, moreover it allows to develop new homological applications of Gröbner basis theory in other areas as noncommutative algebraic geometry and algebraic functional systems. There are available many computational packages that make computations with noncommutative algebras of polynomial type, among them we can mention the following: J. Apel and U. Klaus (http://felix.hgb-leipzig.de); MAS by H. Kredel and M. Pesch (http://krum.rz.uni-mannheim.de/mas.html); Singular: Plural by V. Levandovskyy et al. (http://www.singular.uni-kl.de); Macaulay2 by D. Grayson and M. Stillman (http://www.math.uiuc.edu/Macaulay2); Kan/sm1 by N. Takayama et. al. However, none of the above systems make computations with skew PBW extensions, so the packages developed are useful tools of research for these rings, and in addition, the coefficients of our non commutative polynomials can be in a ring (not necessarily in a field).

During the development of the talk we will describe the `SPBWE.lib` library which consists

of the following packages. The `RingTools` package: This package allows to define the structure of the ring R of coefficients of a skew PBW extension A; The `SPBWETools` package: This is a collection of functions related to the skew PBW extensions, these tools allow to define the structure of a skew PBW extension and perform basic computes with polynomials, operations with vectors or matrices on skew PBW extensions; The `SPBWERings` package: This is constituted by some subclasses of skew PBW extensions that are predefined in the library and with which it is possible to affect computations in the same way as if they had been explicitly defined. The following algebraic structures are predefined into the `SPBWERings` package: additive analogue of Weyl algebras, diffusion algebras, discrete linear algebras, dispin algebras, q-Heisenberg algebras, Manin algebras, mixed algebras, multiplicative analogue of Weyl algebras, PBW extensions, Quasi-Commutative PBW extensions, sigma Ore extensions, univariate skew polynomial rings with injective sigma, Weyl algebras, Witten algebras and Woronowicz algebras. The variety of structures that can be defined is wide and may not only be based on algebra structures but also rings not necessarily algebras. Finally, The `SPBWEGrobner` package: This is a collection of functions related to the Gröbner bases over skew PBW extensions, the main routine included within the package is the version of the left (or right) Buchberger's Algorithm for *bijective* skew PBW extensions. As fundamental hypothesis to use the Gröbner theory in this implementation:
$\diamond$ *We will assume that $A = \sigma(R)\langle x_1, \dots, x_n\rangle$ is a bijective skew PBW extension of a left Gröbner soluble LGS (or right Gröbner soluble RGS) ring R and $Mon(A)$ is endowed with some monomial order.*
In this package was implemented the theory of Gröbner bases and some homological applications. Let A be a skew PBW extension holding the property $\diamond$, then additionally the package includes some functions such as: related to membership problem for left (or right) ideals or modules; to compute the left (or right) module of syzygies of a left (or right) module M; to compute left (or right) inverses of rectangular matrices on A; to compute intersection and quotient for ideals or modules; to compute free resolutions of left A-modules; to compute $\text{Tor}_r^A(M, N)$, where M is a finitely generated centralizing A subbimodule and N is left A-module; to compute $\text{Ext}_A^r(M, N)$, where M is a finitely generated left A-submodule of A^m and N is a finitely generated centralizing A-subbimodule of A^l; to compute if exists of a minimal presentation of a left A-module M; to compute the projective dimension of a left A-module M; and the ably to define iterated skew PBW extensions and perform new computes with these.

We can affirm that the `SPBWE.lib` library is a very useful not only for investigating constructively homological properties of many algebraic structures that can be described as skew PBW extensions, but also for many eventual applications of them.

Keywords
`SPBWE.lib` library, skew PBW extensions, noncommutative computational algebra, homological applications.

References

[1] Acosta, J; Lezama, O., *Universal property of skew PBW extensions,* Algebra Discrete Math. 20 (1), 2015, 1-12
[2] Artamonov V. A., *Derivations of skew PBW extensions*, Commun. Math. Stat., 3 (4), 2015, 449-457.
[3] Bell A; Goodearl K., *Uniform rank over differential operator rings and Poincaré-Birkhoff-Witt extensions*, Pacific J. Math., 131 (1), 1988, 13-37.

[4] FAJARDO, W., *A computational Maple library for skew PBW extensions*, Fundamenta Informaticae, 176, 2019, 159-191.

[5] FAJARDO W; GALLEGO C; LEZAMA O; REYES A; SUÁREZ H; VENEGAS H., *Skew PBW Extensions. Ring and Module-theoretic Properties, Matrix and Gröbner Methods, and Applications*, Algebra and Applications. Springer, Cham, 2020.

[6] FAJARDO, W; LEZAMA, O., *Elementary matrix-computational proof of Quillen-Suslin theorem for Ore extensions,* Fundamenta Informaticae, 164, 2019, 41-59.

[7] FAJARDO, W., *Right Gröbner bases of bijective skew PBW extensions*, Fundamenta Informaticae, 2020, Preprint.

[8] GALLEGO, C., *Matrix computations on projective modules using noncommutative Gröbner bases, Journal of Algebra,* Number Theory: Advances and Applications, 15 (2), 101-139, 2016.

[9] GALLEGO, C., *Filtered-graded transfer of noncommutative Gröbner bases,* Rev. Colombiana Mat. 50 (1), 41-54, 2016.

[10] GALLEGO, C; LEZAMA O., Gröbner bases for ideals of σ-PBW extensions, Comm. Algebra, 39 (1), 2011, 50-75.

[11] GALLEGO, C; LEZAMA O., *Projective modules and Gröbner bases for skew PBW extensions,* Dissertationes Math., 521 (1), 2017, 1-50.

[12] HAMIDIZADEH, M; HASHEMI, E; REYES, A., *A classification of ring elements in skew PBW extensions over compatible rings,* Int. Electron. J. Algebra 28, 75-97 (2020).

[13] HASHEMI, E; KHALILNEZHAD, K; ALHEVAZ, A., (Σ, Δ)*-Compatible Skew PBW Extension Ring,* Kyungpook Math. J. 57 (2017), no. 3, 401-417.

[14] HASHEMI, E; KHALILNEZHAD, K; GHADIRI, M., *Baer and quasi-Baer properties of skew PBW extensions,* J. Algebr. Syst. 7 (2019), no. 1, 1-24.

[15] JIMÉNEZ, H; LEZAMA, O., *Gröbner bases of modules over σ-PBW extensions,* Acta Math. Acad. Paedagog. Nyházi. (N.S.) 32 (2016), 39-66.

[16] LEZAMA, O; GALLEG, C., *d-Hermite rings and skew PBW extensions,* São Paulo J. Math. Sci., **10** (1) (2016), 60-72.

[17] LEZAMA, O; PAIBA, M., *Computing finite presentations of Tor and Ext over skew PBW extensions and some applications,* Acta Math. Acad. Paedagog. Nyházi., 34 (1), 2018.

[18] LEZAMA, O; VENEGAS, H., *Center of skew PBW extensions,* Internat. J. Algebra Comput. 30 (2020), no. 8, 1625-1650.

[19] ORE O., *Theory of Non-Commutative Polynomials*, Ann. of Math. (2), 34 (3), 1933, 480-508.

[20] REYES A; SUÁREZ Y., *On the ACCP in skew Poincaré-Birkhoff-Witt extensions,* Beitr. Algebra Geom. 59 (2018), no. 4, 625-643.

[21] TUMWESIGYE, A; RICHTER, J; SILVESTROV, S., *Centralizers in PBW Extensions.* In: Silvestrov S., Malyarenko A., Rancić M. (eds) Algebraic Structures and Applications. SPAS 2017. Springer Proceedings in Mathematics & Statistics, Vol. 317, Springer, Cham (2020).

[22] B. ZAMBRANO., *Poisson brackets on some skew PBW extensions,* Algebra Discrete Math. 29 (2020), no. 2, 277-302.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Effective Ideal Theory in Commutative and non-Commutative Rings and its Applications"*

Recursive Structures in Involutive Bases Theory

Amir Hashemi[1,2]***, Matthias Orth***[3]***, Werner M. Seiler***[3] [Amir.Hashemi@iut.ac.ir]

[1] Department of Mathematical Sciences, Isfahan University of Technology, Isfahan 84156-83111, Iran

[2] School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, 19395-5746, Iran

[3] Institut für Mathematik, Universität Kassel, Heinrich-Plett-Str. 40, 34132 Kassel, Germany

In this work, we are concerned with *recursive structures* in the theory of involutive bases where the recursion will mainly be over the number of variables in the underlying polynomial ring. The starting point is an old result by Janet providing a recursive criterion for a set of terms to form a Janet basis (see also [2, Corollary 4.11] from where we learned of this result). Let us recall some definitions from involutive bases theory, see [3] for more details. Let $U \subset R = K[x_1, \ldots, x_n]$ be a finite set of terms. For each sequence $d_1, \ldots, d_n$ of non-negative integers and for each index $1 \leq i \leq n$, let

$$U_{[d_i,\ldots,d_n]} = \left\{u \in U \mid \deg_j(u) = d_j,\ i \leq j \leq n\right\} \subseteq U\ . \tag{0.1}$$

The variable x_n is *Janet multiplicative* for $u \in U$, if $\deg_n(u) = \max\{\deg_n(v) \mid v \in U\}$. For $i < n$ the variable x_i is Janet multiplicative for $u \in U_{[d_{i+1},\ldots,d_n]}$, if

$$\deg_i(u) = \max\{\deg_i(v) \mid v \in U_{[d_{i+1},\ldots,d_n]}\}.$$

Let $I \subset R$ be an ideal and $\prec$ a term ordering on R. A Janet head autoreduced subset $G \subset I$ is called a *Janet basis* of I, if for any $f \in I$ there exists $g \in G$ such that $\mathrm{lt}(g) \mid \mathrm{lt}(f)$ and the quotient $\mathrm{lt}(f)/\mathrm{lt}(g)$ contains only Janet multiplicative variables. We first restate and prove Janet's result as a recursive criterion for being a Janet basis, see the next theorem.

Theorem 1. *Let $U = \{t_1, \ldots, t_m\}$ be a finite set of terms. We define $t'_i = t_i|_{x_n=1}$ for all i and $U' = \{t'_1, \ldots, t'_m\} \subset K[x_1, \ldots, x_{n-1}]$. If $\alpha = \max\{\deg_n(t_1), \ldots, \deg_n(t_m)\}$, then we introduce for each degree $\lambda \leq \alpha$ the sets $I_\lambda = \{i \mid \deg_n(t_i) = \lambda\}$ and $U'_\lambda = \{t'_i \mid i \in I_\lambda\}$. Then, U is a Janet basis, if and only if the following two conditions are satisfied:*

1. *For each $\lambda \leq \alpha$, U'_λ is a Janet basis in $K[x_1, \ldots, x_{n-1}]$.*
2. *For each $\beta \leq \lambda < \alpha$, we have $U'_\lambda \subset \langle U'_{\lambda+1}\rangle$.*

As a first extension, we prove a similar recursive criterion for *minimal* Janet bases and use it to provide an algorithm to minimise an arbitrary Janet basis. Currently, the main algorithm for computing a minimal Janet basis is the TQ-algorithm of [4] which determines the basis from scratch. While it is in principle possible to give this algorithm a Janet basis as input, it will not benefit from this (in fact, this is even bad input). By contrast, our novel algorithm efficiently minimises any given Janet basis.

Then we proceed to *Janet-like bases* which where introduced in [5, 6] to obtain more compact bases, in particular in situations where the degrees of the leading terms in some variables differ greatly (as e. g. in toric ideals). Again we will give a recursive criterion for a set to be a (minimal) Janet-like basis. While Gerdt and Blinkov extended solely the Janet division to the Janet-like division, we will introduce the general concept of an involutive-like division and related notions like continuity or constructivity. Our main emphasis will be on Janet-like and Pommaret-like bases and how they are related to each other and to Janet and Pommaret bases. But we will also start developing a syzygy theory for these bases by providing a variant of Schreyer's theorem.

Combining our recursive criteria with a variant of the Buchberger algorithm presented in [1], we develop novel recursive algorithms for the construction of monomial and polynomial Janet and Janet-like bases.

In the second part of this work, we proceed to the construction of Pommaret bases. The *class* of a term x^μ with $\mu = (\mu_1, \ldots, \mu_n)$ is defined as the index $k := \min\{i \mid \mu_i \neq 0\}$. A variable x_i is called Pommaret multiplicative for x^μ, if $i \leq k$. Similar to Janet bases, one can define Pommaret bases as well. Note that an ideal I possesses a finite Pommaret basis if and only if I is in quasi stable position. A monomial ideal $I \subset R$ is called *quasi-stable*, if for any term $u \in I$, for any variable x_k dividing u and for any $i > k$, there exists an exponent $s \geq 0$ such that $x_i^s u/x_k \in I$. A polynomial ideal I is in *quasi-stable position* if $\operatorname{lt}(I)$ (with respect to the degree reverse lexicographical ordering) is quasi-stable. A key issue to study Pommaret bases is to find "good" coordinates, i. e. to transform a given ideal into quasi-stable position (see [7] for an extensive discussion of this topic). We provide the following recursive criteria for being a Pommaret basis.

Theorem 2. *Let $U = \{t_1, \ldots, t_m\}$ be a set of terms. Set $t'_i = t_i|_{x_n=1}$ for each $1 \leq i \leq m$ and $U' = \{t'_1, \ldots, t'_m\}$. Finally, let $\alpha = \max\{\deg(t_1, x_n), \ldots, \deg(t_m, x_n)\}$. For each degree $\lambda \leq \alpha$, we define the index set $I_\lambda = \{i \mid \deg(t_i, x_n) = \lambda\}$ and the set $U'_\lambda = \{t'_i \mid i \in I_\lambda\}$. The given set U is a Pommaret basis, if and only if the following three conditions are satisfied:*

1. *For each $\lambda \leq \alpha$, U'_λ is a Pommaret basis,*
2. *For each $\lambda < \alpha$, we have $U'_\lambda \subset \langle U'_{\lambda+1} \rangle$,*
3. *We have $U \cap K[x_n] = x_n^\alpha$.*

Based on this theorem, we give an effective test for quasi-stability and then a deterministic algorithm for the construction of "good" coordinates. Compared with the results by [7], the novel approach is not only much more efficient, but also the termination proof becomes much simpler. Minor modifications of the underlying ideas lead to recursive criterion for Noether position which also translates immediately into a corresponding deterministic algorithm.

Acknowledgement

The research of the first author was in part supported by a grant from IPM (No. 1400130214).

Keywords
Polynomial ideals, Gröbner bases, involutive bases, Janet bases, Janet-like bases, Pommaret bases, Pommaret-like bases, completion algorithms, recursion, Schreyer's theorem, quasi-stable ideals, Janet trees, Noether position

References

[1] C. Berkesch and F.-O. Schreyer. Syzygies, finite length modules, and random curves. In *Commutative algebra and noncommutative algebraic geometry. Volume I: Expository articles*, pages 25–52. Cambridge: Cambridge University Press, 2015.

[2] M. Ceria. Applications of Bar Code to involutive divisions and a greedy algorithm for complete sets. *arXiv:1910.02802*, pages 1–18, 2019.

[3] V. P. Gerdt and Y. A. Blinkov. Involutive bases of polynomial ideals. *Math. Comput. Simul.*, 45(5-6):519–541, 1998.

[4] V. P. Gerdt and Y. A. Blinkov. Minimal involutive bases. *Math. Comput. Simul.*, 45(5-6):543–560, 1998.

[5] V. P. Gerdt and Y. A. Blinkov. Janet-like Gröbner bases. In *Computer algebra in scientific computing. 8th international workshop, CASC 2005, Kalamata, Greece, September 12–16, 2005. Proceedings*, pages 184–195. Berlin: Springer, 2005.

[6] V. P. Gerdt and Y. A. Blinkov. Janet-like monomial division. In *Computer algebra in scientific computing. 8th international workshop, CASC 2005, Kalamata, Greece, September 12–16, 2005. Proceedings*, pages 174–183. Berlin: Springer, 2005.

[7] A. Hashemi, M. Schweinfurter, and W. M. Seiler. Deterministic genericity for polynomial ideals. *J. Symb. Comput.*, 86:20–50, 2018.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"'Effective Ideal Theory in Commutative and non-Commutative Rings and its Applications"*

Standard bases method for vertex algebras

Pavel Kolesnikov[1], ***Roman Kozlov***[1,2] [pavelsk77@gmail.com]

[1] Sobolev Institute of Mathematics, Novosibirsk, Russia
[2] Mechanics and Mathematics Department, Novosibirsk State University, Novosibirsk, Russia

In this talk we present an approach to the study of combinatorial problems for vertex algebras. The main task is to solve the ideal membership problem in a free vertex algebra. The latter allows us to determine explicitly the Fock space for a vertex algebra defined by generators and relations. As an application, we apply this technique to the study of forgetful functor that turns a vertex algebra into a left-symmetric (pre-Lie) algebra with respect to the normally ordered product.

The theory of vertex algebras (or vertex operator algebras, VOAs) appeared in mathematical physics as an algebraic tool for studying the operator product expansion (OPE) of chiral fields in 2-dimensional conformal field theory which goes back to A. Belavin, A. Polyakov, and A. Zamolodchikov [1]. The algebraic definition of a VOA was first stated by R. Borcherds [2]. The development of the theory of vertex algebras is mainly carried out within the framework of the representation theory. In order to define a vertex algebra in this way, one need to get the base space V, a linear operator $T : V \to V$ (translation), a selected vector $\mathbf{1} \in V$ (vacuum) such that $T\mathbf{1} = 0$, and define a family of vertex operators, formal distributions $Y(a, z) \in gl(V)[[z, z^{-1}]]$, $a \in V$, satisfying certain properties (see, e.g., [3]). The Dong Lemma along with the Goddard Uniqueness Theorem show that it is enough to define the series $Y(a, z)$ not for all $a \in V$, but just for "generators".

In [4], B. Bakalov and V. Kac proposed a bright approach to the definition of a vertex algebra which makes this notion very well fitting into the ordinary algebraic framework. Namely, vertex algebras have become no more "exotic" than, for example, Poisson algebras. A vertex algebra is a unital differential pre-Lie (or left-symmetric) algebra V with a derivation T equipped with a conformal Lie λ-bracket $[\cdot_\lambda \cdot]$ (see [5]) such that these two algebraic structures are related to each other via "quasi-commutativity"

$$a.b - b.a = \int_{-T}^{0} [a_\lambda b]\, d\lambda$$

and “quasi-Leibniz” rule (known as the Wick identity)

$$[a_\lambda(b.c)] = b.[a_\lambda c] + [a_\lambda b].c + \int_0^\lambda [[a_\lambda b]_\mu c]\, d\mu,$$

for all $a, b, c \in V$. Here $x.y$ stands for the product in the pre-Lie algebra V, in terms of vertex operators one has

$$Y(a.b, z) = {:}Y(a, z)Y(b, z){:},$$

the normally ordered product of formal fields (see, e.g., [3]). For example, an associative and commutative differential algebra is a vertex algebra relative to the trivial λ-bracket.

The $\mathbb{Z}_2$-graded version of the definition (vertex superalgebras) is completely analogous modulo the Kaplansky rule.

Free vertex algebras have been introduced and studied in [6], [7]. In order to determine the structure of a vertex algebra defined by generators and relations we need an analogue of the Gröbner bases technique for commutative (differential) algebras. As a convenient language, we choose the presentation of a vertex algebra as a module over an associative algebra.

Let B be a nonempty set presented as a disjoint union $B = B_0 \cup B_1$. Denote by $p(b) \in \{0, 1\}$ the parity of $b \in B$, i.e., $p(b) = i$ iff $b \in B_i$. Given an integer-valued locality function $N : B \times B \to \mathbb{Z}$, a free vertex algebra generated by B is uniquely defined up to isomorphism [6], [7]. Let us restrict the consideration to the case of non-negative locality values, i.e., $N(a, b) \geq 0$ for $a, b \in B$. For $X = \{b(n) \mid b \in B, n \in \mathbb{Z}\}$, denote

$$A_N(B) = \mathbb{C}\Big\langle X \cup \{T\} \mid \sum_{s=0}^{N(a,b)} (-1)^s \binom{N(a,b)}{s} [a(n-s), b(m+s)]_s, \\ Ta(n) + a(n)T + na(n-1), a, b \in B, n, m \in \mathbb{Z}\Big\rangle$$

where $[a(n), b(m)]_s = a(n)b(m) - (-1)^{p(a)p(b)} b(m)a(n)$. Then the $A_N(B)$-module

$$V_N(B) = A_N(B)\text{-mod}\,\langle \mathbf{1} \mid T\mathbf{1},\ a(n)\mathbf{1}, a \in B, n \geq 0\rangle$$

carries a structure of a vertex algebra $\mathcal{F}_N(B)$ which is universal in the class of vertex algebras generated by B with the locality function on B bounded by N.

The key observation is that an ideal in the vertex algebra $\mathcal{F}_N(B)$ is the same as an $A_N(B)$-submodule in $V_N(B)$. Hence, a solution of the ideal membership problem in a free vertex algebra may be solved by means of the Gröbner–Shirshov bases theory for associative algebras [8] and modules [9]. A *standard basis* (or Gröbner–Shirshov basis) in the free vertex algebra $\mathcal{F}_N(B)$ is the Gröbner–Shirshov basis in the left module $V_N(B)$ over the associative algebra $A_N(B)$.

Let Vert, LSym, and LieConf be the categories of vertex, pre-Lie, and Lie conformal algebras, respectively. As follows from the definition, there are two forgetful functors

$$\Phi : \mathrm{Vert} \to \mathrm{LieConf}, \quad \Psi : \mathrm{Vert} \to \mathrm{LSym}.$$

The first one was studied in [6], where the left adjoint functor for Φ was explicitly constructed. Every Lie conformal algebra L embeds into its universal enveloping vertex algebra $V(L)$, and there is an analogue of the Poincaré–Birkhoff–Witt (PBW) Theorem on the linear basis of $V(L)$.

Most of those vertex algebras that appear in applications are obtained either as $V(L)$ for an appropriate Lie conformal algebra L or as a quotient of $V(L)$ modulo the ideal generated by $\mathbf{1} - c$ for a central torsion element $c \in L$. So are the fermion, Heisenberg, Kac–Moody, Virasoro, Weyl vertex algebras (see [3], [10]). We calculate the standard bases for all these examples and show that, in general, the normal form of elements in the universal enveloping vertex algebra $V(L)$ of a Lie conformal algebra L does not depend of the particular multiplication table on L.

The second functor Ψ has completely different properties. We show that there exist pre-Lie (super)algebras that cannot be embedded into a vertex (super)algebra. Namely, let A be a pre-Lie (super)algebra. If A embeds into a vertex (super)algebra in such a way that $a.b = ab$ for all $a, b \in A$ and the locality function on A is bounded then the commutator Lie (super)algebra $A^{(-)}$ is nilpotent. In particular, as follows from the results of [11], a finite-dimensional simple pre-Lie algebra cannot be embedded into a vertex algebra.

This research is supported by Russian Science Foundation (project 21-11-00286).

Keywords
Vertex algebra, Conformal algebra, Left-symmetric algebra, Standard basis

References

[1] A. A. Belavin, A. M. Polyakov, A. B. Zamolodchikov, Infinite conformal symmetry in two-dimensional quantum field theory. *Nuclear Phys.* **241**, 333–380 (1984).
[2] R. E. Borcherds, Vertex algebras, Kac-Moody algebras, and the Monster. *Proc. Nat. Acad. Sci. U.S.A.* **83**, 3068–3071 (1986).
[3] E. Frenkel, D. Ben-Zvi, *Vertex algebras and algebraic curves*. Mathematical Surveys and Monograps **88**. AMS, Providence, RI, 2001.
[4] B. Bakalov, V. G. Kac, Field algebras. *Int. Math. Res. Not.* **3**, 123–159 (2003).
[5] V. G. Kac, *Vertex algebras for beginners, second ed.* University Lecture Series **10**. AMS, Providence, RI, 1998.
[6] M. Roitman, On free conformal and vertex algebras. *J. Algebra* **217**(2), 496–527 (1999).
[7] M. Roitman, Combinatorics of free vertex algebras. *J. Algebra* **255**(2), 297–323 (2002).
[8] L. A. Bokut, Imbeddings into simple associative algebras [Russian]. *Algebra i Logika* **15**, 117–142 (1976).
[9] S.-J. Kang, K.-H. Lee, Gröbner–Shirshov bases for representation theory. *J. Korean Math. Soc.* **37**, 55–72 (2000).
[10] D. Adamović, V. Pedić, On fusion rules and intertwining operators for the Weyl vertex algebra. *J. Math. Phys.* **60**(8), 081701, 18 pp (2019).
[11] D. Burde, Simple left-symmetric algebras with solvable Lie algebra. *Manuscripta Math.* **95**, 397–411 (1998).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Effective Ideal Theory in Commutative and non-Commutative Rings and its Applications"*

Minimum distance bounds on cyclic-skew-cyclic codes

***G. N. Alfarano*[1], *F. J. Lobillo*[2,*], *A. Neri*[3] *and A. Wachter-Zeh*[4]** [jlobillo@ugr.es]

[1] University of Zurich, Switzerland
[2] Universidad de Granada, Spain
[3] Max-Planck-Institute for Mathematics in the Sciences, Leipzig, Germany
[4] Technical University of Munich, Germany

This talk is part of the joint work [1].

Let $\mathbb{E}$ be a field and consider $\mathbb{K}/\mathbb{E}$ and $\mathbb{F}/\mathbb{E}$ extension fields of finite degree, respectively h and m, such that $\mathbb{K} \cap \mathbb{F} = \mathbb{E}$. Moreover, let $\mathbb{L} := \mathbb{F}\mathbb{K}$. Let ℓ be a positive integer and assume that $x^\ell - 1$ splits into linear factors in $\mathbb{K}$, i.e. $\mathbb{K}$ contains all the ℓ-th roots of unity. The field $\mathbb{F}$ will essentially always be the defining field for our linear codes. We assume that $\mathbb{L}/\mathbb{K}$ is a cyclic Galois extension and $\langle \sigma \rangle = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, hence σ has order m. We denote by θ the restriction $\sigma_{|_\mathbb{F}}$ of σ to $\mathbb{F}$ and m is the order of θ, i.e. $\mathrm{Gal}(\mathbb{F}/\mathbb{E}) = \langle \theta \rangle$.

Metrics. In this talk we consider three weights on linear codes. The first one is the well known *Hamming weight* on $\mathbb{F}^\ell$ which is the number of coordinates that are different from 0. i.e.

$$\begin{aligned} \mathrm{wt}_\mathrm{H} : \mathbb{F}^\ell &\longrightarrow \mathbb{N} \\ c &\longmapsto \#\{i : c_i \neq 0\}. \end{aligned}$$

Another well-known metric is the rank metric. Let $\mathbb{F}/\mathbb{E}$ be the field extension defined above and let N be a positive integer. The *rank weight* for $\mathbb{F}/\mathbb{E}$ is defined as the following map:

$$\begin{aligned} \mathrm{wt}_\mathrm{rk}^{\mathbb{F}/\mathbb{E}} : \mathbb{F}^N &\longrightarrow \mathbb{N} \\ c &\longmapsto \dim_\mathbb{E}(\langle c_0, \dots, c_{N-1} \rangle_\mathbb{E}). \end{aligned}$$

The same applies for the extension $\mathbb{L}/\mathbb{K}$. Finally let $n = m\ell$. A given vector $c \in \mathbb{F}^n$, may be partitioned as in (1). The *sum-rank weight* for $\mathbb{F}/\mathbb{E}$ is defined as the function

$$\begin{aligned} \mathrm{wt}_\mathrm{srk}^{\mathbb{F}/\mathbb{E}} : \mathbb{F}^n &\longrightarrow \mathbb{N} \\ c &\longmapsto \textstyle\sum_{i=0}^{\ell-1} \mathrm{wt}_\mathrm{rk}^{\mathbb{F}/\mathbb{E}}(c^{(i)}). \end{aligned}$$

[*] This research was partially funded by AEI (https://doi.org/10.13039/501100011033) grant number PID2019-110525GB-I00.

The canonical way to define a metric from a weight as $\mathrm{d}(u,v) = \mathrm{wt}(u-v)$ for adequate u, v provides three metrics on our linear codes: *Hamming*, *rank* and *sum-rank* metrics denoted as d_{H}, $\mathrm{d}_{\mathrm{rk}}^{\mathbb{F}/\mathbb{E}}$ and $\mathrm{d}_{\mathrm{srk}}^{\mathbb{F}/\mathbb{E}}$ respectively. The minimum Hamming, rank and sum-rank distances of a linear code $\mathcal{C}$ are defined as expected, the minimum corresponding distance between different codewords.

Cyclic-skew-cyclic code. Given $n = m\ell$, any vector $c \in \mathbb{F}^n$, may be partitioned as

$$c = (c^{(0)} \mid \dots \mid c^{(\ell-1)}), \tag{1}$$

where $c^{(i)} = (c_0^{(i)}, \dots, c_{m-1}^{(i)}) \in \mathbb{F}^m$, for every $i \in \{0, \dots, \ell-1\}$.

The *block-shift operator* ρ and the θ*-inblock shift operator* ϕ on $\mathbb{F}^n$ are defined as

$$\rho((c^{(0)} \mid \dots \mid c^{(\ell-1)})) = (c^{(\ell-1)} \mid c^{(0)} \mid \dots \mid c^{(\ell-2)}), \tag{2}$$

$$\phi((c^{(0)} \mid \dots \mid c^{(\ell-1)})) = (\varphi(c^{(0)}) \mid \dots \mid \varphi(c^{(\ell-1)})), \tag{3}$$

where $\varphi : \mathbb{F}^m \to \mathbb{F}^m$ is given by

$$\varphi(v_0, \dots, v_{m-1}) = (\theta(v_{m-1}), \theta(v_0), \dots, \theta(v_{m-2})).$$

Definition 1 ([2]). A code $\mathcal{C} \subseteq \mathbb{F}^n$ is called *cyclic-skew-cyclic* if $\rho(\mathcal{C}) = \mathcal{C}$ and $\phi(\mathcal{C}) = \mathcal{C}$.

As usual, the skew polynomial ring $\mathbb{F}[z;\theta]$ is built from the relation $za = \theta(a)z$. Setting up $\theta(x) = x$ we get an isomorphism $\theta : \mathbb{F}[x] \to \mathbb{F}[x]$ and we can build $\mathbb{F}[x][z;\theta]$. It follows $z^m - 1$ is a central polynomial and $\langle z^m - 1\rangle$, the left ideal generated by $z^m - 1$, is a two-sided ideal. Since $\theta(x^\ell - 1) = x^\ell - 1$, θ factors to an automorphism of $\mathbb{F}[x]/\langle x^\ell - 1\rangle$. Define

$$\mathcal{S}' = \frac{\mathbb{F}[x]}{\langle x^\ell - 1\rangle}, \quad \mathcal{R}' = \frac{\mathcal{S}'[z;\theta]}{\langle z^m - 1\rangle},$$

Proposition 2. There exists a canonical isomorphisms of rings

$$\mathcal{R}' \cong \frac{\mathbb{F}[x][z;\theta]}{\langle z^m - 1, x^\ell - 1\rangle}.$$

Whenever the characteristic of $\mathbb{F}$ does not divide ℓ, $\mathcal{R}'$ is semisimple.

The natural identification given by the map $\nu : \mathbb{F}^n \longrightarrow \mathcal{R}'$, defined as

$$\nu((c^{(0)} \mid \dots \mid c^{(\ell-1)})) = \sum_{j=0}^{m-1} \left(\sum_{i=1}^{\ell} c_j^{(i)} x^i \right) z^j, \tag{4}$$

lead to the arithmetic characterization of cyclic-skew-cyclic codes.

Theorem 3 ([2,Theorem 1]). Let $\mathcal{C} \subseteq \mathbb{F}^n$ be a code. The following are equivalent.

1. $\mathcal{C}$ is a cyclic-skew-cyclic code.
2. $\nu(\mathcal{C})$ is a left ideal of $\mathcal{R}'$.

Evaluation and defining sets. Evaluation in $\mathcal{R}'$ can be done with the aid of Proposition 2 and the inclusion $\mathbb{F}[x][z;\theta] \subseteq \mathbb{L}[x][z;\sigma]$.

Lemma 4. Let $\beta, b \in \mathbb{L}$ and $f = \sum_i \sum_j a_{ij} x^i z^j \in \mathbb{L}[x][z,\sigma]$. Then

$$f - \sum_i \sum_j a_{ij} b^i N_j(\beta) \in \langle x - b, z - \beta \rangle$$

where $N_j(\beta) = \beta\sigma(\beta)\cdots\sigma^{j-1}(\beta)$ is the truncated jth-norm of β.

Given $a \in \mathbb{K}$ and $\alpha \in \mathbb{L}^*$ a non zero element, the evaluation map can be defined applying the lemma to $\beta = \sigma(\alpha)\alpha^{-1}$ and a as

$$\mathrm{Ev}_{\alpha,a}\left(\sum_{i,j} a_{ij} z^i x^j\right) = \sum_i \sum_j a_{ij} a^i \sigma^j(\alpha)\alpha^{-1}.$$

Since $z - \beta \mid z^m - 1$ and $x - a \mid x^\ell - 1$, this map factorizes through $\mathcal{R}'$.

Definition 5. Let $\mathcal{C} \subseteq \mathcal{R}'$ be a cyclic-skew-cyclic code. Then, the *defining set* $T_\mathcal{C}$ of $\mathcal{C}$ is the set

$$T_\mathcal{C} = \{(a,\alpha) \in \mathbb{K} \times \mathbb{L}^* \mid a^\ell = 1, \mathrm{Ev}_{a,\alpha}(c(x,z)) = 0 \; \forall c \in \mathcal{C}\}.$$

The main Theorems prove the Hartman-Tzeng and the Roos bounds for cyclic-skew-cyclic codes.

Theorem 6. (Sum-Rank HT bound) Let $n = m\ell$ and $\mathcal{C} \subseteq \mathbb{F}^n$ be a cyclic-skew-cyclic code. Let b, δ, r, t_1, t_2 be integers, such that $\gcd(n, t_1) = 1$, $\gcd(n, t_2) < \delta$. Let $a \in \mathbb{K}$ be a primitive ℓ-th root of unity and α be a normal element of $\mathbb{L}/\mathbb{K}$. If

$$\{(a^{b+it_1+st_2}, \sigma^{it_1+st_2}(\alpha)) \in \mathbb{K} \times \mathbb{L}^* \mid 0 \leq i \leq \delta - 2, 0 \leq s \leq r\} \subseteq T_\mathcal{C},$$

then $\mathrm{d}_{\mathrm{srk}}(\mathcal{C}) \geq \delta + r$.

Theorem 7. (Sum-rank Roos bound) Let $n = m\ell$ and $\mathcal{C} \subseteq \mathbb{F}^n$ be a cyclic-skew-cyclic code. Let $b, s, \delta, k_0, \ldots, k_r$ be integers, such that $\gcd(n, s) = 1$, $k_i < k_{i+1}$ for $i = 0, \ldots, r-1$, $k_r - k_0 \leq \delta + r - 2$. Let $a \in \mathbb{K}$ be a primitive ℓ-th root of unity and α be a normal element of $\mathbb{L}/\mathbb{K}$. If

$$\{(a^{b+si+k_j}, \sigma^{si+k_j}(\alpha)) \in \mathbb{K} \times \mathbb{L}^* \mid 0 \leq i \leq \delta - 2, 0 \leq j \leq r\} \subseteq T_\mathcal{C},$$

then $\mathrm{d}_{\mathrm{srk}}(\mathcal{C}) \geq \delta + r$.

Keywords
Cyclic-skew-cyclic code, Sum-rank metric, Hartman-Tzeng bound, Roos bound.

References

[1] G. N. ALFARANO; F. J. LOBILLO; A. NERI; A. WACHTER-ZEH, Sum-rank product codes and bounds on the minimum distance. `arXiv:2105.15086 [cs.IT]`, 2021.
[2] U. MARTÍNEZ-PEÑAS, Sum-rank BCH codes and cyclic-skew-cyclic codes. `arXiv:2009.04949`, 2020.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Effective Ideal Theory in Commutative and non-Commutative Rings and its Applications"*

Recovery from Power Sums

Hana Melánová[1]***, Bernd Sturmfels***[2,3]***, Rosa Winter***[2] [hana.melanova@univie.ac.at]

[1] Faculty of Mathematics, University of Vienna, Austria
[2] Max Planck Institute for Mathematics in the Sciences, Leipzig, Germany
[3] Statistics and Computer Science University of California at Berkeley

The aim of this talk is to present a case study in solving systems of polynomial equations, for a model setting that is reminiscent of signal processing applications. We are interested in the problem of recovering n points from the evaluation of m power sums. More precisely, let us suppose there is a secret list of complex numbers $z_1, z_2, \ldots, z_n$. These z_i are unknown and our task is to find them. Measurements are made by evaluating the m powers sums

$$\sum_{i=1}^{n} z_i^{a_j} = c_j,$$

where $\mathcal{A} = \{a_1, a_2, \ldots, a_m\}$ is a set of m distinct positive integers. Our goal is to recover $z = (z_1, \ldots, z_n)$ from $c = (c_1, \ldots, c_m)$. We address the following two questions:

(Q1): Is a recovery possible? (Q2): If yes, is the recovery unique?

To model this problem, for any given pair $(n, \mathcal{A})$, we consider the polynomial map

$$\phi_{\mathcal{A},\mathbb{C}} \colon \mathbb{C}^n \to \mathbb{C}^m, \quad \text{where } \phi_j \;=\; x_1^{a_j} + x_2^{a_j} + \cdots + x_n^{a_j} \qquad \text{for } j = 1, 2, \ldots, m. \tag{1}$$

In order to answer the questions (Q1) and (Q2), we investigate the image and the fibers of the map $\phi_{\mathcal{A},\mathbb{C}}$, or equivalently, study the following polynomial system of m equations in n variables:

$$\phi_{\mathcal{A}}(\underline{x}) \;=\; \underline{c}, \tag{2}$$

where $\underline{x} = (x_1, \ldots, x_n)$ and $\underline{c} = (c_1, \ldots, c_m)$.

We distinguish three different cases. If $m > n$, then (2) is in general overconstrained and has no solutions. However, if (2) comes from measurements, i.e., $\underline{c} = \phi_{\mathcal{A},\mathbb{C}}(\underline{z})$, for some $\underline{z} \in \mathbb{C}^n$, in general we expect a unique recovery of $\{z_1, \ldots, z_n\}$. If $m < n$, then (2) is underconstrained and the solution set is an algebraic variety, in general of dimension $n - m$. Finally, there is the square case $m = n$ for which, in general, (2) has finitely many solutions, namely at most as many as the Bézout number $a_1 a_2 \cdots a_n$ suggests.

Let us illustrate the three cases on an example:

Example 1 ($n = 3$). a) Consider that measurements with $\mathcal{A} = \{2, 4, 5, 10\}$ were done for the secret numbers $\{-7, 26, 50\}$. Then the system (2) equals

$$\begin{aligned} &x_1^2 + x_2^2 + x_3^2 = 3225, && x_1^5 + x_2^5 + x_3^5 = 324364569, \\ &x_1^4 + x_2^4 + x_3^4 = 6709377, && x_1^{10} + x_2^{10} + x_3^{10} = 97797417378128625. \end{aligned} \tag{3}$$

For the graded reverse lexicographic order with $x_1 > x_2 > x_3$, the Gröbner basis equals

$$\{x + y + z - 69, y^2 + yz + z^2 - 69y - 69z + 768, (z - 50)(z - 26)(z + 7)\}$$

and spans a zero-dimensional radical ideal whose solution set consists of precisely 6 solutions. Hence, the set $\{-7, 26 - 50\}$ is recovered uniquely.

b) As next we consider the system given by only the first three equations of (3), i.e., the system corresponding to the measurements $\mathcal{A} = \{2, 4, 5\}$. This system does not allow a unique recovery of $\{-7, 26, 50\}$ anymore as it has 36 complex solutions. Notice further, that the number of solutions here is strictly less than the Bézout number $40 = 2 \cdot 4 \cdot 5$.

c) Finally, making only two measurements with $\mathcal{A} = \{2, 5\}$ is obviously not sufficient for a unique recovery because the first two equations of (3) define a one-dimensional curve.

The questions (Q1) and (Q2) become interesting already when the secret numbers $z_1, \ldots, z_n$ are real or even positive. In the latter case, the problem of recovery from power sums is equivalent to the following problem: Assume a secret vector $v \in \mathbb{R}^n_{\geq 0}$ is given. We do not know the vector but we know its length w.r.t. m different p-norms on $\mathbb{R}^n$. Is the vector v uniquely determined by them? Hence, we investigate also the maps (and their fibers and images) $\phi_{\mathcal{A},\mathbb{R}}$ and $\phi_{\mathcal{A},\geq 0}$ that are obtained by restricting $\phi_{\mathcal{A},\mathbb{C}}$ to $\mathbb{R}^n$ and $\mathbb{R}^n_{\geq 0}$, respectively.

Another and very interesting problem is the study of the behaviour of the maps $\phi_{\mathcal{A},\mathbb{C}}$, $\phi_{\mathcal{A},\mathbb{R}}$, and $\phi_{\mathcal{A},\geq 0}$ in special points. In non-generic points, the fibers do not need necessarily to behave as expected. Either their dimension/cardinality can drop or it can jump up drastically as illustrated in the following example.

Example 2. Instead of (3) we consider the modified system of equations given by

$$\begin{aligned} &x_1^2 + x_2^2 + x_3^2 = 0, && x_1^5 + x_2^5 + x_3^5 = 0, \\ &x_1^4 + x_2^4 + x_3^4 = 0, && x_1^{10} + x_2^{10} + x_3^{10} = 0. \end{aligned} \tag{4}$$

a) Remarkably, if we consider only the first three equations of (4) corresponding to the power set $\mathcal{A} = \{2, 4, 5\}$, we do not obtain only finitely many complex points as its solution set. This system has a one-dimensional solution set that is given by the union of the lines spanned by the vectors $(1, \zeta, \zeta^2)$ and $(\zeta^2, \zeta, 1)$, where ζ is a primitive cubic root of unity.

b) Moreover, the solution set remains the same one-dimensional variety if we consider the full system (4).

Notice that in the case $n = m$, the system (2) with $\underline{c} = 0$ has finitely many solutions if and only if the corresponding power sums form a regular sequence. The complete classification of the power sets $\mathcal{A}$ defining regular sequences is widely open even for $n = 3$. However, Conca, Krattenthaler and Watanabe give a conjecture for $n = 3$ [1, Conjecture 2.10].

In this talk, we will give results and further open problems concerning recovery from power sums. We will on the one hand focus on the square case $n = m$, where we will present supporting computational evidence as well as a generalization of [1, Conjecture 2.10]. On the other hand, we will discuss the uniqueness of recovery in the case $m = n + 1$. Finally, we will discuss what is known about the ramification locus of $\phi_{\mathcal{A},\mathbb{C}}$, which can be described in terms of Schur polynomials, and we give a description of the branch locus for $m = 3$.

Keywords
Power sums, Regular sequences, Bézout number

References

[1] A. Conca, C. Krattenthaler, J. Watanabe, Regular sequences of symmetric polynomials. *Rend. Semin. Mat. Univ. Padova* **121**, 179–199 (2009).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Effective Ideal Theory in Commutative and non-Commutative Rings and its Applications"*
(organized by M. Ceria, A. Leroy, T. Mora)

On the computation of syzygies via multivariate matrix multiplication

Simone Naldi[1]***, Vincent Neiger***[1] [simone.naldi@unilim.fr]

[1] Univ. Limoges, CNRS, XLIM, UMR 7252 F-87000 Limoges, France

In this document, $\mathcal{R}$ denotes the the ring $\mathbb{K}[X_1, \dots, X_r]$ of r-variate polynomials over a field $\mathbb{K}$, and for an integer n, then $\mathcal{R}^n$ denotes the free $\mathcal{R}$-module of polynomial vectors of length n: elements in $\mathcal{R}^n$ are represented as row vectors in our notation.

We are given an $\mathcal{R}$-submodule $\mathcal{N} \subset \mathcal{R}^n$, with the assumption that $\mathcal{R}^n/\mathcal{N}$ has finite dimension as a $\mathbb{K}$-vector space, we denote D such dimension. Let $\boldsymbol{F} \in \mathcal{R}^{m\times n}$ be a polynomial matrix, with rows $\boldsymbol{f}_1, \dots, \boldsymbol{f}_m \in \mathcal{R}^n$.

The main question we are concerned with is the characterization of algebraic relations, also known as syzygies, of the rows of $\boldsymbol{F}$. More precisely, we consider the first syzygy module of $\boldsymbol{F}$ modulo $\mathcal{N}$, that is the set

$$\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F}) = \{\boldsymbol{p} = (p_i)_{1\le i\le m} \in \mathcal{R}^m \mid \boldsymbol{pF} = \textstyle\sum_{1\le i\le m} p_i \boldsymbol{f}_i \in \mathcal{N}\},$$

where $\boldsymbol{p}$ is seen as a $1\times m$ row vector. The goal is to compute a $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$, with respect to some prescribed term order $\preccurlyeq$ on $\mathcal{R}^m$ (possibly induced from a term order on $\mathcal{R}^n$). Note that $\mathcal{R}^m/\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$ has dimension at most D, as a $\mathbb{K}$-vector space. The problem of computing the module of syzygies is a central question in commutative algebra, for instance it is the basic step in the computation of free resolutions.

Following a path of work pioneered by Marinari, Möller and Mora [1,2,3], we focus on the specific situation where the module $\mathcal{N}$ is described using duality: it is known as the vanishing locus of D linear functionals $\varphi_j : \mathcal{R}^n \to \mathbb{K}$, that is

$$\mathcal{N} = \bigcap_{1\le j\le D} \ker(\varphi_j).$$

In this context, it is customary to make a regularity assumption equivalent to the following: $\mathcal{N}_i = \cap_{1\le j\le i} \ker(\varphi_i)$ is an $\mathcal{R}$-module, for $1 \le i \le D$ (see e.g. Alg. 2 in [2] or Eqn. (4.1) in [4] or Eqn. (5) in [5] for such assumptions and related algorithms).

This assumption allows one to design algorithms which compute Gröbner bases of $\mathrm{Syz}_{\mathcal{N}_i}(\boldsymbol{F})$ iteratively for increasing i, until reaching $i = D$ and obtaining the sought basis of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$. An efficient such iterative procedure is given in Alg. 2 in [2].

The context we have just described specializes to some well-known problems in computer algebra. One of these, of particular interest, is when $\mathcal{N}$ is the vanishing ideal of a given set of points, that is $n = 1$, and $\mathcal{N} \subset \mathcal{R}$ is the ideal of all polynomials vanishing at prescribed points $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_D \in \mathbb{K}^r$. In this contexts, the linear functionals are evaluations:

$$\varphi_j(f) = f(\boldsymbol{\alpha}_j) \in \mathbb{K}.$$

The question is, given the points, m polynomials as $\boldsymbol{F} \in \mathcal{R}^{m \times 1}$, and a monomial order $\preccurlyeq$, to compute a $\preccurlyeq$-Gröbner basis of the set of vectors $\boldsymbol{p}$ such that $\boldsymbol{pF}$ vanishes at all the points. When $m = 1$ and $\boldsymbol{F} = [1]$, this means computing a $\preccurlyeq$-Gröbner basis of the ideal of the points, as studied in [2,3].

Another case is that of (multivariate) Padé approximation and its extensions, as studied for instance in [4,5], as well as in the context of multidimensional linear recurrence relations [6]. The basic setting is for $n = 1$, with $\mathcal{N} = \langle X_1^{d_1}, \ldots, X_r^{d_r} \rangle$, and $\boldsymbol{F} = [\begin{smallmatrix} f \\ -1 \end{smallmatrix}]$ for some given $f \in \mathcal{R}$. Then, elements of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$ are vectors $(q, p) \in \mathcal{R}^2$ such that $f = p/q \bmod X_1^{d_1}, \ldots, X_r^{d_r}$. Here, the $D = d_1 \cdots d_r$ linear functionals correspond to the coefficients of multidegree less than $(d_1, \ldots, d_r)$; note that not all orderings of these functionals satisfy the assumption above.

For these two situations, as well as some extensions of them, the fastest known algorithms rely on linear algebra and have a cost bound of $O(mD^2 + rD^3)$ operations in $\mathbb{K}$ [2,4], recently improved in [7] to $O(mD^{\omega-1} + rD^{\omega}\log(D))$ where $\omega < 2.38$ is the exponent of matrix multiplication.

Based on work in [9,10], in the specific case of an ideal of points $\mathcal{N}$ and the lexicographic order, Ceria and Mora gave a combinatorial algorithm to compute the $\preccurlyeq_{\mathrm{lex}}$-monomial basis of $\mathcal{R}/\mathcal{N}$, the Cerlienco-Mureddu correspondence, and squarefree separators for the points using $O(rD^2\log(D))$ operations [11].

In this talk we describe a recent contribution to this topic, which is partly published in [8]. We propose a divide and conquer algorithm for the problem of computing a $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$ in the multivariate case. This is based on the iterative algorithm in [2], observing that each step of the iteration can be interpreted as a left multiplication by a matrix which has a specific shape, which we call elementary Gröbner basis. The new algorithm reorganizes these matrix products through a divide and conquer strategy, and groups several products by elementary Gröbner bases into a single multivariate polynomial matrix multiplication.

A drawback of our approach when compared to [2] is that the new algorithm does not explicitly compute Gröbner bases for all intermediate syzygy modules $\mathrm{Syz}_{\mathcal{N}_i}(\boldsymbol{F})$. By computing less, we expect to achieve better computational complexity. This potential gain of complexity is explicit in the case of multivariate matrix Padé approximation.

For $\mathcal{R} = \mathbb{K}[X, Y]$, let $f_1, \ldots, f_m \in \mathcal{R}$, and let $\preccurlyeq$ be a monomial order on $\mathcal{R}$. Then the algorithm in [8] can compute a minimal $\preccurlyeq$-Gröbner basis of the module of Hermite-Padé approximants

$$\{(p_1,\ldots,p_m)\in\mathcal{R}^m \mid p_1f_1+\cdots+p_mf_m=0 \bmod \langle X^d,Y^d\rangle\}$$

using $O\tilde{}(m^\omega d^{\omega+2})$ field operations, where $O\tilde{}(\cdot)$ means that polylogarithmic factors are omitted.

In this case the vector space dimension is $D=d^2$. Thus, as noted above and to the best of our knowledge, the fastest previously known algorithm for this task has a cost of $O\tilde{}(md^{2(\omega-1)}+d^{2\omega})$ operations in $\mathbb{K}$ and does not exploit fast polynomial multiplication.

Keywords
Syzygies; Gröbner basis; divide and conquer; matrix multiplication; Padé approximation;

References

[1] M.E. ALONSO, M.G. MARINARI, T. MORA. *The Big Mother of all Dualities: Möller Algorithm*. Communications in Algebra 31, 2 (2003), 783–818.
[2] M.G. MARINARI, H. M. MÖLLER, T. MORA. *Gröbner bases of ideals defined by functionals with an application to ideals of projective points*. Appl. Algebra Engrg. Comm. Comput. 4, 2 (1993), 103–145.
[3] H.M. MÖLLER AND B. BUCHBERGER. *The Construction of Multivariate Polynomials with Preassigned Zeros*. In EUROCAM'82 (LNCS), Vol. 144. Springer, 24–31.
[4] P. FITZPATRICK. *Solving a Multivariable Congruence by Change of Term Order*. J. Symb. Comput. 24, 5 (1997), 575–589.
[5] H. O'KEEFFE, P. FITZPATRICK. *Gröbner basis solutions of constrained interpolation problems*. Linear Algebra Appl. 351 (2002), 533–551.
[6] J. BERTHOMIEU, J.-C. FAUGÈRE. *A Polynomial-Division-Based Algorithm for Computing Linear Recurrence Relations*. In Proceedings of ISSAC 2018. 79–86.
[7] V. NEIGER, É. SCHOST. *Computing syzygies in finite dimension using fast linear algebra*. Journal of Complexity, Volume 60, October 2020, 101502.
[8] S. NALDI, V. NEIGER. *A Divide-and-conquer Algorithm for Computing Gröbner Bases of Syzygies in Finite Dimension*. In Proceedings of ISSAC 2020. 380–387.
[9] L. CERLIENCO, M. MUREDDU. *From algebraic sets to monomial linear bases by means of combinatorial algorithms*. Discrete Mathematics 139, 1-3 (1995), 73–87.
[10] B. FELSZEGHY, B. RÁTH, L. RÓNYAI. *The lex game and some applications*. J. Symb. Comput. 41, 6 (2006), 663–681.
[11] M. CERIA, T. MORA. *Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game*, Preprint arXiv:1805.09165.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Effective Ideal Theory in Commutative and non-Commutative Rings and its Applications”*

Computing syzygies in finite dimension using fast linear algebra

Vincent Neiger[1]***, Éric Schost***[2] [vincent.neiger@unilim.fr]

[1] Univ. Limoges, CNRS, XLIM, UMR 7252, F-87000 Limoges, France
[2] University of Waterloo, Waterloo ON, Canada

This talk presents results from [8,9].

Let $\mathbb{K}$ be a field and consider the polynomial ring $\mathbb{K}[\mathbf{X}] = \mathbb{K}[X_1, \ldots, X_r]$; the set of $m \times n$ matrices over a ring $\mathcal{R}$ is denoted by $\mathcal{R}^{m\times n}$. We are interested in the efficient computation of relations, known as syzygies, between elements of a $\mathbb{K}[\mathbf{X}]$-module $\mathcal{M}$.

Let us write the $\mathbb{K}[\mathbf{X}]$-action on $\mathcal{M}$ as $(p, f) \in \mathbb{K}[\mathbf{X}] \times \mathcal{M} \mapsto p \cdot f$, and let $f_1, \ldots, f_m$ be in $\mathcal{M}$. Then, for a given monomial order $\prec$ on $\mathbb{K}[\mathbf{X}]^m$, we want to compute the Gröbner basis of the kernel of the homomorphism

$$\begin{array}{rcl} \mathbb{K}[\mathbf{X}]^m & \to & \mathcal{M} \\ (p_1, \ldots, p_m) & \mapsto & p_1 \cdot f_1 + \cdots + p_m \cdot f_m. \end{array}$$

This kernel is called the *module of syzygies* of $(f_1, \ldots, f_m)$ and written $\mathrm{Syz}_{\mathcal{M}}(f_1, \ldots, f_m)$.

In this talk, we focus on the case where $\mathcal{M}$ has finite dimension D as a $\mathbb{K}$-vector space; as a result, the quotient $\mathbb{K}[\mathbf{X}]^m / \mathrm{Syz}_{\mathcal{M}}(f_1, \ldots, f_m)$ has dimension at most D as a $\mathbb{K}$-vector space. Then one may adopt a linear algebra viewpoint detailed in the next paragraph, where the elements of $\mathcal{M}$ are seen as row vectors of length D and the multiplication by the variables is represented by so-called multiplication matrices. This representation was used and studied in [2,7,1,4], mainly in the context where $\mathcal{M}$ is a quotient $\mathbb{K}[\mathbf{X}]/\mathcal{I}$ for some ideal $\mathcal{I}$ (thus zero-dimensional of degree D) and more generally a quotient $\mathbb{K}[\mathbf{X}]^n/\mathcal{N}$ for some submodule $\mathcal{N} \subseteq \mathbb{K}[\mathbf{X}]^n$ with $n \in \mathbb{N}_{>0}$. This representation with multiplication matrices allows one to perform computations in such a quotient via linear algebra operations.

Assume we are given a $\mathbb{K}$-vector space basis $\mathcal{F}$ of $\mathcal{M}$. For i in $\{1, \ldots, r\}$, the matrix of the structure morphism $f \mapsto X_i \cdot f$ with respect to this basis is denoted by $\mathbf{M}_i$; this means that for f in $\mathcal{M}$ represented by the vector $\mathbf{f} \in \mathbb{K}^{1\times D}$ of its coefficients on $\mathcal{F}$, the coefficients of $X_i \cdot f \in \mathcal{M}$ on $\mathcal{F}$ are $\mathbf{f}\mathbf{M}_i$. We call $\mathbf{M}_1, \ldots, \mathbf{M}_r$ *multiplication matrices*; note that they are pairwise commuting. The data formed by these matrices defines the module $\mathcal{M}$ up to isomorphism; we use it as a representation of $\mathcal{M}$. For p in $\mathbb{K}[\mathbf{X}]$ and for f in $\mathcal{M}$ represented by the vector $\mathbf{f} \in \mathbb{K}^{1\times D}$ of its coefficients on $\mathcal{F}$, the coefficients of $p \cdot f \in \mathcal{M}$ on $\mathcal{F}$ are $\mathbf{f}\, p(\mathbf{M}_1, \ldots, \mathbf{M}_r)$; hereafter this vector is written $p \cdot \mathbf{f}$. From this point of view, syzygy modules can be described as follows.

Definition. For m and D in $\mathbb{N}_{>0}$, let $\mathbf{M} = (\mathbf{M}_1, \ldots, \mathbf{M}_r)$ be pairwise commuting matrices in $\mathbb{K}^{D\times D}$, and let $\mathbf{F} \in \mathbb{K}^{m\times D}$. Denoting by $\mathbf{f}_1, \ldots, \mathbf{f}_m$ the rows of $\mathbf{F}$, for $\mathbf{p} = (p_1, \ldots, p_m) \in \mathbb{K}[\mathbf{X}]^m$ we write

$$\mathbf{p} \cdot \mathbf{F} = p_1 \cdot \mathbf{f}_1 + \cdots + p_m \cdot \mathbf{f}_m = \mathbf{f}_1\, p_1(\mathbf{M}) + \cdots + \mathbf{f}_m\, p_m(\mathbf{M}) \in \mathbb{K}^{1\times D}.$$

The *syzygy module* $\mathrm{Syz}_{\mathbf{M}}(\mathbf{F})$, whose elements are called syzygies for $\mathbf{F}$, is defined as

$$\mathrm{Syz}_{\mathbf{M}}(\mathbf{F}) = \{\mathbf{p} \in \mathbb{K}[\mathbf{X}]^m \mid \mathbf{p} \cdot \mathbf{F} = \mathbf{0}\};$$

as noted above, $\mathbb{K}[\mathbf{X}]^m / \mathrm{Syz}_{\mathbf{M}}(\mathbf{F})$ has dimension at most D as a $\mathbb{K}$-vector space. □

In particular, if in the above context $\mathbf{F}$ is the matrix of the coefficients of $f_1, \ldots, f_m \in \mathcal{M}$ on the basis $\mathcal{F}$, then $\mathrm{Syz}_{\mathbf{M}}(\mathbf{F}) = \mathrm{Syz}_{\mathcal{M}}(f_1, \ldots, f_m)$. In this talk we present a fast algorithm to solve the following problem.

Input:
- a monomial order $\prec$ on $\mathbb{K}[\mathbf{X}]^m$,
- pairwise commuting matrices $\mathbf{M} = (\mathbf{M}_1, \ldots, \mathbf{M}_r)$ in $\mathbb{K}^{D\times D}$,
- a matrix $\mathbf{F} \in \mathbb{K}^{m\times D}$.

Output: the reduced $\prec$-Gröbner basis of $\mathrm{Syz}_{\mathbf{M}}(\mathbf{F})$.

The obtained complexity bound is in $O(mD^{\omega-1} + rD^{\omega}\log(D))$, improving upon results presented in [6,3,5].

In the above problem the multiplication matrices $\mathbf{M}_1, \ldots, \mathbf{M}_r$ are assumed to be known, yet in some cases such as the change of monomial ordering, one will first need to compute these matrices from a known reduced $\prec$-Gröbner basis. In this talk we will also describe an efficient algorithm to compute the multiplication matrices under suitable assumptions on the shape of the staircase associated with the input $\prec$-Gröbner basis.

Keywords
Gröbner basis, Syzygies, Complexity, Fast linear algebra

References

[1] Alonso, M.E., Marinari, M.G., Mora, T., 2003. The Big Mother of all Dualities: Möller Algorithm. Communications in Algebra 31, 783–818.

[2] Auzinger, W., Stetter, H.J., 1988. An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations, in: Proceedings Numerical Mathematics 1988, Birkhäuser Basel, Basel. pp. 11–30.

[3] Faugère, J.C., Gianni, P., Lazard, D., Mora, T., 1993. Efficient computation of zero-dimensional Gröbner bases by change of ordering. Journal of Symbolic Computation 16, 329–344.

[4] Kehrein, A., Kreuzer, M., Robbiano, L., 2005. An algebraist's view on border bases, in: and Dickenstein, A., Emiris, I.Z. (Eds.), Solving Polynomial Equations: Foundations, Algorithms, and Applications. Springer, pp. 169–202.

[5] Marinari, M.G., Möller, H.M., Mora, T., 1993. Gröbner bases of ideals defined by functionals with an application to ideals of projective points. Appl. Algebra Engrg. Comm. Comput. 4, 103–145.

[6] Möller, H.M., Buchberger, B., 1982. The construction of multivariate polynomials with preassigned zeros, in: EUROCAM'82, Springer.

[7] Mourrain, B., 1999. A new criterion for normal form algorithms, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Springer Berlin Heidelberg, Berlin, Heidelberg. pp. 430–442.

[8] Neiger, V., 2016. Bases of relations in one or several variables: fast algorithms and applications. Ph.D. thesis. École Normale Supérieure de Lyon.
URL: https://tel.archives-ouvertes.fr/tel-01431413/

[9] Neiger, V., Schost, É. Computing syzygies in finite dimension using fast linear algebra, Journal of Complexity, Volume 60, 2020.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Effective Ideal Theory in Commutative and non-Commutative Rings and its Applications”*

Type IV Codes over non unitary rings

Patrick Solé [1], [patrick.sole@telecom-paris.fr]

[1] I2M, CNRS, Marseille, France

There are exactly 11 rings of order 4, four of which are unital by Rhagavandran (1969). Among the remaining seven we select three as alphabets for our codes: E,I, H. We study quasi self-dual codes and Type IV codes over these rings, two special kinds of self-orthogonal codes. E is non-commutative and local, and leads to invariant theory of weight enumerators. I is commutative local and leads to a mass formula. H is commutative semi-local and allows classification under permutation equivalence. The build up construction is studied over E,I, and H. Joint works with *Adel Alahmadi, Amani Alkhatiry, Alaa Altassan, Widyan Bassafar, Alexis Bonnecaze, Hatoon Shoaib*.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Effective Ideal Theory in Commutative and non-Commutative Rings and its Applications”*

Subalgebras in $K[x]$ of small codimension

Rode Grönkvist[1]***, Anna Torstensson, Victor Ufnarovski***[1] [victor.ufnarovski@math.lth.se]

[1] Centre for Mathematical Science, Lunds Institute of Technology, Lunds University, Lund, Sweden

Let K be an algebraically closed field of zero characteristic and A be a subalgebra in $K[x]$ of finite codimension $n > 0$.

We want to introduce the following definition, which we consider to be very useful.

The Subalgebra spectrum S of subalgebra A consists of such $\alpha \in K$ that either $f'(\alpha) = 0$ for any $f(x) \in A$ or there exists $\beta \neq \alpha$ such that $f(\alpha) = f(\beta)$ for any $f(x) \in A$. In the second case β obviously belongs to the spectrum as well.

Theorem 1. *Each proper subalgebra A in $K[x]$ has non-empty spectrum of size not greater than $2n$.*

The subalgebra spectrum allows easy to construct SAGBI bases and to classify subalgebras of small codimensions.

Here is an example of classification of subalgebras of codimension 2.

If we call the vector of degrees in SAGBI basis of an algebra A the type of A the n we can describe all such subalgebras in the following way.

Theorem 2. *Let A be a subalgebra of codimension 2. Then it either has type $(2, 5)$ or type $(3, 4, 5)$. The spectrum contains $s \leq 4$ elements and depending of its size we have the following possibilities.*

s=1 $A = \{f(x)|f'(\alpha) = 0; af''(\alpha) + bf'''(\alpha) = 0\}$.
$a = 0, b \neq 0$ in case $(2, 5)$ and $a \neq 0$ in case $(3, 4, 5)$.

s=2 $A = \{f(x)|f(\alpha) = f(\beta); af'(\alpha) + bf'(\beta) = 0\}$.
$a = b \neq 0$ in case $(2, 5)$ and $a \neq b$ in case $(3, 4, 5)$.

s=2 $A = \{f(x)|f'(\alpha) = f'(\beta) = 0\}$.
This is possible only in the case $(3, 4, 5)$.

s=3 $A = \{f(x)|f(\alpha) = f(\beta); f'(\gamma) = 0\}$;
$\alpha + \beta = 2\gamma$ in case $(2, 5)$, $\alpha + \beta \neq 2\gamma$ in case $(3, 4, 5)$.

s=3 $A = \{f(x)|f(\alpha) = f(\beta) = f(\gamma)\}$.
This is possible only in the case $(3, 4, 5)$.

s=4 $A = \{f(x)|f(\alpha) = f(\beta); f(\gamma) = f(\delta)\}$.
$\alpha + \beta = \gamma + \delta$ in case $(2, 5)$ and $\alpha + \beta \neq \gamma + \delta$ in case $(3, 4, 5)$.

Here $\alpha, \beta, \gamma, \delta$ are different elements of the spectrum.

For larger codimension the condition become more exotic. Here is an example:

Theorem 3. *If algebra A of codimension 3 has a spectrum consisting of single element α then A is one of the following algebras*

1. $A = \{f(x)|f'(\alpha) = f''(\alpha) = af'''(\alpha) + bf^{(4)}(\alpha) + cf^{(5)}(\alpha) = 0\}$.
If $a \neq 0$ then type is (4,5,6,7) and for $a = 1$ the SAGBI basis is:
$$(x - \alpha)^4 - 4b(x - \alpha)^3, (x - \alpha)^5 - 20c(x - \alpha)^3, (x - \alpha)^6, (x - \alpha)^7.$$
If $a = 0$ and $b \neq 0$ then type is (3,5,7) and for $b = 1$ the SAGBI basis is:
$$(x - \alpha)^3, (x - \alpha)^5 - 5c(x - \alpha)^4, (x - \alpha)^7.$$
For $a = b = 0, c \neq 0$ type is (3,4) and the SAGBI basis is
$$(x - \alpha)^3, (x - \alpha)^4.$$
If $a = b = c = d = 0$ the codimension is 2.

2. $A = \{f(x)|f'(\alpha) = f'''(\alpha) + 3af''(\alpha) = f^{(5)}(\alpha) + 10af^{(4)}(\alpha) + df''(\alpha) = 0\}$.
with $a \neq 0$. If $d \neq 0$ then type is (4,5,6,7) and the SAGBI basis is:
$$d(x - \alpha)^4 - 120(x - \alpha)^3 + 120a(x - \alpha)^2,$$
$$ad(x - \alpha)^5 - 60(x - \alpha)^3 + 60a(x - \alpha)^2, (x - \alpha)^6, (x - \alpha)^7.$$
If $d = 0$ then then type is (3,5,7) and the SAGBI basis is:
$$(x - \alpha)^3 - a(x - \alpha)^2, 2a(x - \alpha)^5 - (x - \alpha)^4, (x - \alpha)^7.$$

3. $A = \{f(x)|f'(\alpha) = f'''(\alpha) = cf^{(5)}(\alpha) + df''(\alpha) = 0\}$. *If $d \neq 0$ then type is (4,5,6,7) and the SAGBI basis is:*
$$(x - \alpha)^4, d(x - \alpha)^5 - 60c(x - \alpha)^2, (x - \alpha)^6, (x - \alpha)^7.$$
If $c \neq 0, d = 0$ then type is (2,7) and the SAGBI basis is:
$$(x - \alpha)^2, (x - \alpha)^7.$$
If $c = 0, d = 0$ we get codimension 2.

The monomial subalgebras have a spectrum consisting of zero only and an easy description.

Theorem 4. *Let A be a* ***monomial subalgebra****, thus A is spanned over K by monomials $\{x^s, s \in S\}$, where S is a numerical semigroup. Then $f(x) \in A$ if and only if $f^{(i)}(0) = 0$ for each i that does not belong to S.*

Here is another example of classification.

Theorem 5. *Any proper subalgebra A of finite index in $K[x]$ containing a polynomial $q(x)$ of degree two has a spectrum consisting of $g > 0$ elements for some g. The spectrum has $k = \left[\frac{g}{2}\right]$ pairs $\{\alpha_i, \beta_i\}$, $i = 1, \ldots, k$ such that for each i the sum $\alpha_i + \beta_i$ has a constant value $2\alpha_0$ and (for odd g) one extra element, namely $\alpha_0 (= \beta_0)$. For each $0 \leq i \leq k$ there exists numbers $m_i \geq 0$ such that $f(x) \in A$ if and only if*

- $f^{(j)}(\alpha_i) = (-1)^j f^{(j)}(\beta_i)$ *for each $0 < i \leq k$ and each $0 \leq j \leq m_i$,*
- $f^{(j)}(\alpha_0) = 0,\ j = 1, 3, \ldots, 2m_0 - 1$ *(for odd g only).*

Vice versa, if an algebra satisfies such conditions, then it is generated by

$$(x - \alpha_0)^2,\ (x - \alpha_0)^{2m_0+1} \prod_{i \geq 1} (x - \alpha_i)^{m_i+1} (x - \beta_i)^{m_i+1}.$$

There are many interesting open questions connected to the spectrum which we plan to discuss.

Keywords
SAGBI basis, Subalgebra spectrum,

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Effective Ideal Theory in Commutative and non-Commutative Rings and its Applications"*

On Gröbner bases over Tate Algebras

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

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

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

Tate series are naturally approximated by multivariate polynomials over $\mathbb{F}_p$ or $\mathbb{Z}/p^n\mathbb{Z}$, and it is possible to define a theory of Gröbner bases for ideals of Tate series, which opens the way towards effective rigid geometry. In this talk, I will present those definitions, as well as different algorithms to compute Gröbner bases for Tate series.

Keywords
Algorithms, Power series, p-adic numbers, Tate algebra, Gröbner bases, F5 algorithm, FGLM, p-adic precision

References

[1] X. Caruso; T. Vaccon; T. Verron, Gröbner bases over Tate algebras. In *International Symposium on Symbolic and Algebraic Computation (ISSAC) 2019*, 74–81. Association for Computing Machinery, New York, NY, USA, 2019.
[2] X. Caruso; T. Vaccon; T. Verron, Signature-based algorithms for Gröbner bases over Tate algebras. In *International Symposium on Symbolic and Algebraic Computation (ISSAC) 2020*, 70–77. Association for Computing Machinery, New York, NY, USA, 2020.
[3] X. Caruso; T. Vaccon; T. Verron, On FGLM Algorithms With Tate Algebras. On arXiv:2102.03339

S5. Computer Algebra Modeling in Science and Engineering

Organized by

Alexander Prokopenya and Haiduke Sarafian

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Computer Algebra Modeling in Science and Engineering"*

Evolution Equations of Translational-Rotational Motion of an Axisymmetric Satellite with Variable Oblate

Saltanat Bizhanova[1] [bizhanova.saltanat92@gmail.com]

[1] Faculty of Mechanical and Mathematics, Al-Farabi Kazakh National University, Almaty, Kazakstan

The long-term evolution of translational-rotational motion of an axisymmetric satellite with variable oblate in the central gravitational field are obtained. Newton's interaction force is characterized by an approximate expression of the force function up to the second harmonic. The body masses vary isotropically at different rates. The axes of the own coordinate system of the nonstationary axisymmetric body are directed along the principle axes of inertia of the body and we assumed that in the course of evolution their relative orientation remains unchanged. Doing necessary symbolic computations, we obtain the equations of motion of the satellite in terms of the canonical osculating Delaunay-Andoyer elements. Using the methods of canonical perturbation theory, a particular case of the problem is investigated in detail, when the reactive forces and additional torques are equal to zero. Equations of the translational-rotational motion of the satellite in osculating analogues of Delaunay-Andoyer elements are described. Equation of motion consists of twelve nonautonomous first-order equations that are canonical. In the case when there is no resonance, the evolutionary equation is obtained by double averaging according to the Gaussian scheme. The evolutionary equation decomposes into a system of four first-order differential equations with one first integral, the solution of which determines the evolution of the system. On the basis of these equations establish some qualitative analysis of motion. All necessary symbolic calculations are performed using the Wolfram Mathematica computer algebra system.

Keywords
translational-rotational motion, an axisymmetric satelite, evolution equation

References

[1] M. Minglibayev, *Dynamics of Gravitating Bodies with Variable Masses and Sizes*. LAMBERT Academic, Germany, 2012.
[2] S. Bizhanova; M. Minglibayev; A. Prokopenya, A Study of Secular Perturbations of Translational-Rotational Motion in a Nonstationary Two-Body Problem Using Computer Algebra. *Computational Mathematics and Mathematical Physics* **60**(1), 26–35 (2020).
[3] G. Duboshin, *Celestial Mechanics: Basic Problems and Methods*. Nauka, Moscow, 1975.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Computer Algebra Modeling in Science and Engineering"*

Non-Generic Case of Leap-Frog Algorithm for Optimal Knots Selection in Fitting Reduced Data

Ryszard Kozera[1,2]***, Lyle Noakes***[2] [ryszard_kozera@sggw.edu.pl]

[1] Institute of Information Technology, Warsaw University of Life Sciences - SGGW, Warsaw, Poland
[2] School of Physics, Mathematics and Computing, The University of Western Australia, Perth, Australia

The problem of fitting $n + 1$ points $\mathcal{M} = \{x_i\}_{i=0}^n$ in arbitrary Euclidean space $\mathbb{E}^m$ is discussed here. The class $\mathcal{I}$ of piecewise C^2 interpolants $\gamma : [0, T] \to \mathbb{E}^m$ satisfying $\gamma(t_i) = x_i$ and $\ddot{\gamma}(t_0) = \ddot{\gamma}(T) = \vec{0}$ admits the *internal knots* $\mathcal{T} = \{t_i\}_{i=1}^{n-1}$ to *vary* satisfying the inequalities $t_0 = 0 < t_1 < ... < t_n = T$. We also stipulate that $\gamma \in \mathcal{I}$ is at least of class C^1 over $\mathcal{T}$ and extends to $C^2([t_i, t_{i+1}])$. Recall that for any fixed set of knots $\mathcal{T}$ the minimization task (over $\mathcal{I}$):

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

yields a unique optimal curve $\gamma_{opt} \in \mathcal{I}$ rendering *a natural cubic spline* γ_{NS} - see [1] or [2]. Consequently, letting the knots $\{t_i\}_{i=1}^{n-1}$ to vary, the task of optimizing (1) over $\mathcal{I}$ reformulates into a search for an optimal natural spline γ_{NS} with knots $\{t_i\}_{i=1}^{n-1}$ relaxed subject to $t_i < t_{i+1}$. By [1], as γ_{NS} is uniquely determined by $\mathcal{T}$, minimizing (1) converts into minimizing a highly non-linear function $J_0(t_1, t_2, \ldots, t_{n-1})$ depending on $n - 1$ variables satisfying $t_0 = 0 < t_1 < ... < t_n = T$. Majority of numerical schemes for finding critical points of J_0 lead to numerical difficulties (see e.g. [3]). We discuss here *a Leap-Frog scheme* (see [3] or [4]) which minimizes J_0 based on optimizing a sequence of single variable functions $J_0^{(k)}(t_{k+1})$. The analysis of the sufficient conditions enforcing *unimodality* of $J_0^{(k)}$ for the generic case of Leap-Frog iterations (over each internal sub-interval $[t_i, t_{i+2}]$ with $i = 1, \ldots, n-3$) is addressed in [5]. Our paper extends the latter to the non-generic case of Leap-Frog optimizations taking place over two terminal sub-intervals $[0, t_2]$ and $[t_{n-2}, T]$. Symbolic calculation and numerical tests accompany the theoretical analysis in question.

Keywords
Interpolation, optimization, reduced data

References

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

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

[3] R. KOZERA; L. NOAKES, Optimal knots selection for sparse reduced data. In *Image and Video Technology - PSIVT 2015 Workshops*, F. Huang and A. Sugimoto, 3–14., LNCS 9555, Springer Int. Pub., Switzerland, 2016.

[4] L. NOAKES; R. KOZERA, Nonlinearities and noise reduction in 3-source photometric stereo. *Journal of Mathematical Imaging and Vision* **18**(2), 119–124 (2003).

[5] R. KOZERA; L. NOAKES; A. WILIŃSKI, Generic case of Leap-Frog algorithm for optimal knots selection in fitting reduced data. In *Computational Sciences - ICCS 2021*, M. Paszyński et al., 337–350., LNCS 12745 Part IV, Springer Nature Switzerland AG, Cham Switzerland, 2021.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Computer Algebra Modeling in Science and Engineering”*

On Dynamic Equilibrium of a Swinging Atwood Machine and Its Stability

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

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

The swinging Atwood machine (SAM) consists of two masses $m_1, m_2 = m_1(1+\varepsilon)$ attached to opposite ends of a massless inextensible thread wound round two massless frictionless pulleys of negligible radius (see [1,2]). The mass m_2 is constrained to move only along a vertical while mass m_1 is allowed to oscillate in a plane and it moves like a pendulum of variable length. Such a system has two degrees of freedom and its Hamiltonian function may be written in the form

$$\mathcal{H} = \frac{p_r^2}{2(2+\varepsilon)} + \frac{p_\varphi^2}{2r^2} + (1+\varepsilon)r - r\cos\varphi, \tag{1}$$

where two variables r, φ describe geometrical configuration of the system, and p_r, p_φ are the corresponding canonically conjugate momenta. Note that equations of motion of the SAM are essentially nonlinear, and their general solution cannot be found in symbolic form. However, there exists a periodic solution which may be represented in the form of power series in a small parameter ε (see [3])

$$\begin{aligned} r(t) = 1 + \frac{\varepsilon}{16}(1 - 6\cos(2t)) - \frac{3\varepsilon^2}{2048}\left(87 - 92\cos(2t) + 35\cos(4t)\right) + \\ + \frac{\varepsilon^3}{131072}\left(4275 - 8166\cos(2t) + 5067\cos(4t) - 1510\cos(6t)\right), \quad (2) \\ \varphi(t) = \sqrt{\varepsilon}\left(2\sin t + \frac{53\varepsilon}{192}\sin(3t) + \frac{\varepsilon^2}{81920}\left(14795\sin t - 8495\sin(3t) + 5813\sin(5t)\right)\right). \end{aligned}$$

Note that for $\varepsilon > 0$ the system under consideration has no a static equilibrium state when the coordinates $r(t), \varphi(t)$ are some constants. As periodic solution (2) describes oscillations of the bodies near some equilibrium positions and such a state of the system exists only owing to oscillations one can consider this state as a state of dynamic equilibrium.

As the amplitude of oscillations in (2) is determined by the masses difference ε, it is quite natural to investigate stability of solution (2). Analysing differential equations of the perturbed motion of the SAM and using an infinite determinant method (see [4]), we computed the characteristic exponents in the form of power series

$$\sigma_{1,2} = \pm i, \;\; \sigma_{3,4} = \pm i \frac{\sqrt{3\varepsilon}}{2} \left(1 - \frac{17\varepsilon}{32} + \frac{85\varepsilon^2}{256} \right). \tag{3}$$

Note that characteristic exponents (3) are different purely imaginary numbers. Thus we prove that periodic solution (2) is stable in linear approximation.

Keywords
Swinging Atwood machine, periodic motion, characteristic exponents, stability

References

[1] N.B. TUFILLARO, T.A. ABBOTT, D.J. GRIFFITHS, Swinging Atwood's machine. *American Journal of Physics* **52**(10), 895–903 (1984).
[2] A.N. PROKOPENYA, Motion of a swinging Atwood's machine: simulation and analysis with Mathematica. *Mathematics in Computer Science* **11**(3), 417–425 (2017).
[3] A.N. PROKOPENYA, Construction of a periodic solution to the equations of motion of generalized Atwood's machine using computer algebra. *Programming and Computer Software* **46**(2), 120–125 (2020).
[4] A.N. PROKOPENYA, Determination of the stability boundaries for the hamiltonian system with periodic coefficients. *Mathematical Modelling and Analysis* **10**(2), 191–204 (2005).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Computer Algebra Modeling in Science and Engineering"*

Alternate Cooling Model verse Newton's Cooling

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

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

It is customary to applying Newton's cooling as the standard model investigating the time dependency of temperature of a hot substance exposed to a cool ambient. The rate of change of heat in Newton's model is simplistically related to linear-temperature difference of the two [1,2,3]. In our research flavored investigation we consider a fresh model, cooling that depends to the difference of temperature-squared conducive to similar results. Utilizing a Computer Algebra System (CAS), especially Mathematica [4,5] we show the equivalency of the two.

Keywords
Newton's cooling, alternate cooling model, Wolfram Mathematica

References

[1] https://www.math24.net/newtons-law-cooling.
[2] http://amsi.org.au/ESA-Senior-Years/SeniorTopic3/3e/3e-4history-3.html.
[3] https://byjus.com/jee/newtons-law-of-cooling.
[4] STEPHEN WOLFRAM, *Mathematica "A general computer software system and language intended for mathematical and other applications"*,V12.0, Wolfram Research, 2019.
[5] http://Wolfram.com, (2020) Mathematica V12.1.1.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Computer Algebra Modeling in Science and Engineering"*

What Projective Angle Makes the Arc-Length of the Trajectory in a Resistive Media Maximum? A reverse engineering approach

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

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

We consider the motion of a massive point-like projectile thrown with initial velocity with respect to horizontal in a two dimensional vertical plane under the influence of gravity in a viscose media. Two different velocity-dependent resistive media models are considered – linear and quadratic. With an objective to utilizing a Computer Algebra System (CAS), specifically Mathematica [1] numerically we solve the corresponding equations of motions. For a set of compatible parameters characterizing viscose forces graphically we display comparing the trajectories explicitly showing the impact of the models. Utilizing the model-dependent trajectory equations numerically we evaluate their associated arc-lengths. What distinguishes our approach vs. the existing body of work is the notion of the "reverse engineering". Meaning, utilizing our numeric data we establish their corresponding analytic counter parts. Ultimately, utilizing both output numerically and analytically we determine the matching initial projectile angles maximizing their respective arc-lengths.

Keywords
Projectile motion, resistive media, reverse engineering, Wolfram Mathematica

References

[1] STEPHEN WOLFRAM, *Mathematica "A general computer software system and language intended for mathematical and other applications"*, V12.0, Wolfram Research, 2019.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Computer Algebra Modeling in Science and Engineering”*

Creating Various Materials for Remote Lectures with TeX, KeTCindy and Computer Algebra Systems

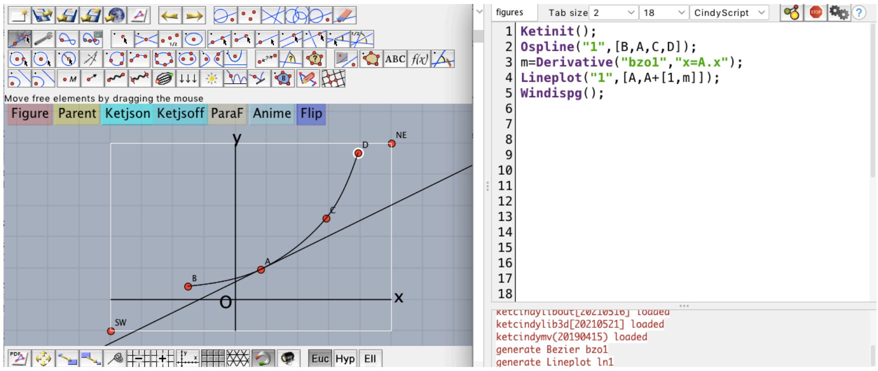
***S. Takato*[1]*, N. Hamaguchi*[2]*, K. Nishiura*[3]*, S. Yamashita*[4]** [takato@phar.toho-u.ac.jp]

[1] KeTCindy Center, Magnolia Inc.
[2] National Institute of Technology, Nagano College
[3] National Institute of Technology, Fukushima College
[4] National Institute of Technology, Kisarazu College

COVID-19 has drastically changed the style of mathematics classes at college level. Many teachers often use presentation slides instead of black/white boards. However, comparing with the latter tools, the formers have several problems that need to be overcome:

(1) to display mathematical expressions without frustration.
(2) to use figures, free curves in particular, freely.
(3) to put components in the most suitable position.
(4) to display expressions step by step.

Although (1) of the above is the main reason almost all mathematics teachers use TeX, there probably aren’t so many teachers who have a good command of (2) and (3). These are weaknesses of TeX itself. We began to develop KETpic/KETCindy since 2006 to compensate them. KETpic was a macro package of Maple, Mathematica and Scilab, whereas KETCindy, current version, is that of R and Cinderella. The followings are screens of Cinderella.



```
Ketinit();
Ospline("1",[B,A,C,D]);
m=Derivative("bzo1","x=A.x");
Lineplot("1",[A,A+[1,m]]);
Windispg();
```

```
ketcindylibout[20210516] loaded
ketcindylib3d[20210521] loaded
ketcindymv(20190415) loaded
generate Bezier bzo1
generate Lineplot ln1
```

Fig. 1 Cindy screen and Cindy script editor

As a simple example, we demonstrate steps to draw a Bézier curve and its tangent.

(1) Put points A,B,C,D on Cindy screen(see Fig.1).

(2) Write the following scripts in the script editor:

```
Ospline("1",[B,A,C,D]);
m=Derivative("bzo1","x=A.x");
Lineplot("1",[A,A+[1,m]]);
```

(3) Press button ’Figure’ on Cindy screen, then the left of Fig.2 will be obtained.

(4) Add other accesories as the right of Fig.2.

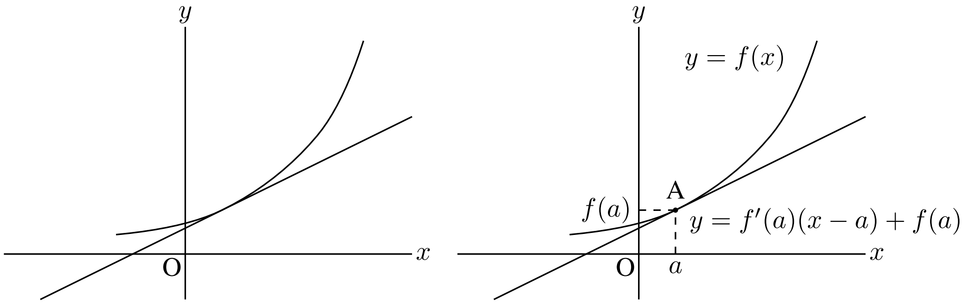
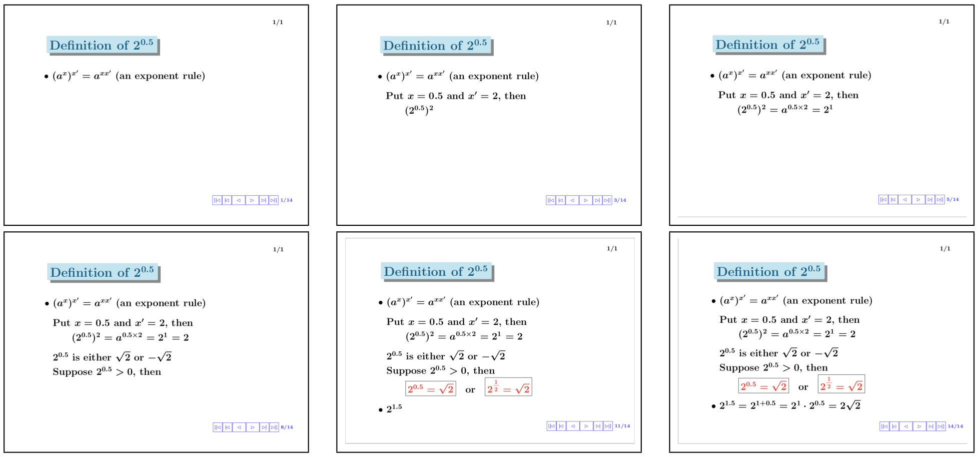


Fig.2 Bézier curve with the tangent

Here, ’layer environment’ we have developed is used for page layout as follows. This is our solution for problem (3).

```
\begin{layer}{140}{0}
\putnotese{3}{2}{\scalebox{0.6}{\input{fig/bezier1.tex}}}
\putnotese{68}{2}{\scalebox{0.6}{\input{fig/bezier2.tex}}}
\end{layer}
```

We have also added the function to produce TEX presentation slides to KETCindy, which supports step-by-step displays.



1/1

Definition of $2^{0.5}$

- $(a^x)^{x'} = a^{xx'}$ (an exponent rule)

1/14

1/1

Definition of $2^{0.5}$

- $(a^x)^{x'} = a^{xx'}$ (an exponent rule)

Put $x = 0.5$ and $x' = 2$, then
$(2^{0.5})^2$

3/14

1/1

Definition of $2^{0.5}$

- $(a^x)^{x'} = a^{xx'}$ (an exponent rule)

Put $x = 0.5$ and $x' = 2$, then
$(2^{0.5})^2 = a^{0.5\times 2} = 2^1$

5/14

1/1

Definition of $2^{0.5}$

- $(a^x)^{x'} = a^{xx'}$ (an exponent rule)

Put $x = 0.5$ and $x' = 2$, then
$(2^{0.5})^2 = a^{0.5\times 2} = 2^1 = 2$

$2^{0.5}$ is either $\sqrt{2}$ or $-\sqrt{2}$
Suppose $2^{0.5} > 0$, then

8/14

1/1

Definition of $2^{0.5}$

- $(a^x)^{x'} = a^{xx'}$ (an exponent rule)

Put $x = 0.5$ and $x' = 2$, then
$(2^{0.5})^2 = a^{0.5\times 2} = 2^1 = 2$

$2^{0.5}$ is either $\sqrt{2}$ or $-\sqrt{2}$
Suppose $2^{0.5} > 0$, then
$\boxed{2^{0.5} = \sqrt{2}}$ or $\boxed{2^{\frac{1}{2}} = \sqrt{2}}$

- $2^{1.5}$

11/14

1/1

Definition of $2^{0.5}$

- $(a^x)^{x'} = a^{xx'}$ (an exponent rule)

Put $x = 0.5$ and $x' = 2$, then
$(2^{0.5})^2 = a^{0.5\times 2} = 2^1 = 2$

$2^{0.5}$ is either $\sqrt{2}$ or $-\sqrt{2}$
Suppose $2^{0.5} > 0$, then
$\boxed{2^{0.5} = \sqrt{2}}$ or $\boxed{2^{\frac{1}{2}} = \sqrt{2}}$

- $2^{1.5} = 2^{1+0.5} = 2^1 \cdot 2^{0.5} = 2\sqrt{2}$

14/14

Fig.3 Slide page divided into 14

We remark each page should be divided into as many pieces as possible and the number of characters in the page should be reduced considering the educational effect at college level.

KETCindy can call Maxima from inside and use the result in the subsequent Cindy scripts. As an example, we demonstrate to find finite continued fractions of $\zeta(3)$. Maxima has functions `bfzeta` to get numerical value of $\zeta(s)$ and `cfa` to get continued fraction representation, so we only write the following Cindy scripts.

```
cmdL=[
 "z:bfzeta(3,10)",[],
 "c:cfa(z)",[],
 "z::c",[]
];
CalcbyM("ans",cmdL,[""]);
```

The result `ans` is a list of strings like

```
[[1.202056903b0,[1,4,1,18,1,1,1,4,1,9,9,2,1,2,5,1,1,1,27]]
```

Using the next formula, we can obtain the sequence of finite conitinued fractions $\{\frac{p_n}{q_n}\}$.

$$p_n = a_n p_{n-1} + p_{n-2},\ q_n = a_n q_{n-1} + q_{n-2} \tag{1}$$

The scripts are as follows.

```
aL=parse(ans_2);
cvL=[];
pm1=1; pm2=0; qm1=0; qm2=1;
forall(0..10,nn,
 p=aL_(nn+1)*pm1+pm2;
 q=aL_(nn+1)*qm1+qm2;
 cvL=concat(cvL,[[p,q]]);
 pm2=pm1; pm1=p; qm2=qm1; qm1=q;
);
```

The result is:

```
[1,1],[5,4],[6,5],[113,94],[119,99],[232,193],[351,292],...
```

Remark

Recently, KETCindy has become to be able to call Wolfram Engine for Developers(WE) as well. Using this, scripts are simpler, as WE has `Convergents` to get finite conitinued fractions directly.

```
cmdL2=[
 "z=N[Zeta[3]]",[],
 "c=Convergents[z,10]",[],
 "c",[]
];
CalcbyW("ans",cmdL2);
```

The result is:

```
{1,5/4,6/5,113/94,119/99,232/193,351/292,1636/1361,...}
```

Moreover, KETCindy has the function to create an HTML file using `CindyJS`.

https://cindyjs.org

For example, the HTML of Fig.1 can be obtained only by (1) creating the original HTML from Cindy menu and (2) pressing button `Ketjsoff` on Cindy screen.

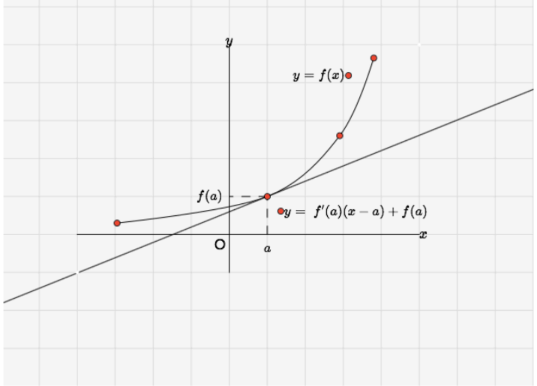


Fig.4 an HTML display of the first example

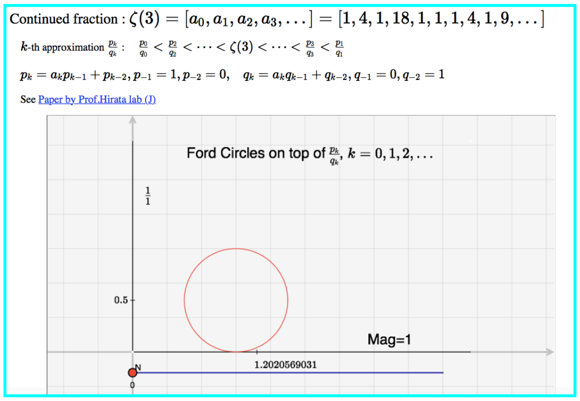
We have uploaded the file at

`https://s-takato.github.io/ketcindysample/forpapers/`.

Students can move the elements interactively with their own device such as a smartphone, iPad, PC and so on. They need no other softwares except for a browser , so these HTML,whose size is so small, will be useful in remote classes. Other various samples will be found at

`https://s-takato.github.io/ketcindysample/`.

The last example is an HTML of Ford Circles of finite continuous fractions of $\zeta(3)$.



Continued fraction : $\zeta(3) = [a_0, a_1, a_2, a_3, \dots] = [1, 4, 1, 18, 1, 1, 1, 4, 1, 9, \dots]$

k-th approximation $\frac{p_k}{q_k}$: $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < \zeta(3) < \cdots < \frac{p_3}{q_3} < \frac{p_1}{q_1}$

$p_k = a_k p_{k-1} + p_{k-2}, p_{-1} = 1, p_{-2} = 0, \quad q_k = a_k q_{k-1} + q_{k-2}, q_{-1} = 0, q_{-2} = 1$

See Paper by Prof.Hirata lab (J)

Ford Circles on top of $\frac{p_k}{q_k}$, $k = 0, 1, 2, \dots$
$\frac{1}{1}$
0.5
Mag=1
1.2020569031
N
0

Fig.5 Ford Circles

Click inside Fig.5, then the HTML will appear.

References

[1] S.Takato, *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 –*. ICMS 2016, LNCS **9725**, 371–379, Springer, 2016.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Computer Algebra Modeling in Science and Engineering"*

On the Equilibria and Bifurcations of a Rotating Double Pendulum

Jonathan Tot[1], ***Robert H. Lewis***[2] [jonathan.tot@dal.ca]

[1] Department of Mathematics and Statistics, Dalhousie University, Halifax, NS
[2] Mathematics Department, Fordham University, Bronx, NY

The double pendulum, a simple system of classical mechanics, is widely studied as an example of, and testbed for, chaotic dynamics. In [1], Maiti et al. study a generalization of the simple double pendulum with equal point-masses at equal lengths, to a rotating double pendulum, fixed to a coordinate system uniformly rotating about the vertical. In this work, we study a further generalization: a rotating double pendulum constructed from *physical* pendula, or rigid 3D bodies. We examine what equilibrium configurations exists for the system across a comparatively large parameter space, as well as what bifurcations occur in those equilibria. Elimination algorithms are employed to reduce systems of polynomial equations, which allows for equilibria to be visualized, and also to demonstrate which models within the parameter space exhibit bifurcation. We find the `DixonEDF` algorithm for the Dixon resultant[2], written in the computer algebra system *Fermat*, to be capable to complete the computation for the challenging system of equations that represents bifurcation, while attempts with other algorithms were terminated after several hours.

Keywords
Double Pendulum, Bifurcation, Polynomial System Solving, Elimination, Dixon Resultant

References

[1] S. Maiti et al., Nonlinear dynamics of a rotating double pendulum. *Physics Letters A* **380**, 408–412 (2016).
[2] R.H. Lewis, Dixon-EDF: The Premier Method for Solution of Parametric Polynomial Systems. In *Applications of Computer Algebra. ACA 2015. Springer Proceedings in Mathematics & Statistics, vol 198*, I. Kotsireas, E. Martínez-Moro (eds.), 237-256. Springer, Cham, 2017.

S7. Computer Algebra in Coding Theory and Cryptography (CACT)

Organized by

Edgar Martinez-Moro and Irene Marquez-Corbella

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Computer Algebra in Coding Theory and Cryptography"*

Resolution of the Conjecture on Exceptional APN Function When the First and the Second Terms Have Odd Degrees

Carlos Agrinsoni[1]***, Heeralal Janwa***[1]***, Moises Delgado***[2]
[{carlos.agrinsoni,heeralal.janwa,moises.delgado}@upr.edu]

[1] Department of Mathematics
University of Puerto Rico at Rio Piedras
17 University Ave. Ste 1701 San Juan PR, 00925-2537
[2] Mathematics Physics
University of Puerto Rico Cayey
205 Calle Antonio R. Barcelo, Cayey, 00736

An almost perfect non-linear (APN) function on $\mathbb{F}_{2^n}$ is one whose directional derivative on nonzero elements is at most two to one. The APN functions have applications in coding theory, cryptography, and sequence designs. A function that is APN over $\mathbb{F}_{2^n}$ and also on infinitely many extensions is called an exceptional APN function. Janwa and Wilson, Janwa, McGuire and Wilson, Jedlicka, and finally McGuire and Hernando in 2011 [1] proved that the exceptional APN monomials up to CCZ equivalence are the Gold $f(x) = x^{2^k+1}$ and Kasami-Welch $f(x) = x^{2^{2k}-2^k+1}$ monomials. Aubrey, McGuire, and Rodier [5] conjectured that up to CCZ equivalence, the only exceptional APN functions are the ones from these two families of monomials. They also established that the odd degrees are necessarily the Gold or Kasami-Welch exponents. For the converse, substantial progress has been made by Delgado and Janwa [3, 4], and Ferard [2] when the degree of the second term is odd. Only a few exceptions remain in the literature for these cases. Here we present proofs for the remaining cases and thus establish a resolution of this conjecture. We deduce our results as a consequence of our recent theorems and algorithms for absolute irreducibility testing of multivariate polynomials over finite fields. These absolute irreducibility results are of considerable importance in applications of computer algebra in coding theory and cryptography.

References

[1] Hernando, Fernando; McGuire, Gary, *Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions*, Journal of Algebra, 2011

[2] Férard, Eric, *A infinite class of Kasami functions that are not APN infinitely often*, Contemp. Math., Vol. 686, pag. 45–63, 2017

[3] Delgado, Moises; Janwa, Heeralal, *Some new results on the conjecture on exceptional APN functions and absolutely irreducible polynomials: the Gold case*, Advances in Mathematics of Communications, 2017

[4] Delgado, Moises; Janwa, Heeralal, *On the absolute irreducibility of hyperplane sections of generalized Fermat varieties in $\mathbb{P}^3$ and the conjecture on exceptional APN functions: the Kasami-Welch degree case*, 2016

[5] Aubry, Yves; McGuire, Gary; Rodier, François, *A few more functions that are not APN infinitely often*, Finite fields: theory and applications, Amer. Math. Soc., Providence, RI, 2010

Two and Three Weight Codes via Our GU Codes

***Eddie A. Arrieta*, Heeralal Janwa** [{eddie.arrieta,heeralal.janwa}@upr.edu]

Department of Mathematics
University of Puerto Rico at Rio Piedras
17 University Ave. Ste 1701 San Juan PR, 00925-2537

Linear codes with few weights have applications in cryptography, association schemes, designs, strongly regular graphs, finite group theory, finite geometries, among other disciplines. For two weight codes, see [4] , for three and few weights codes [5], [6], and [7]. We use our GU code construction to obtain two-weight, three-weight and few-weights linear codes. Consequently, we also give elementary constructions of two-weight codes in Calderbank and Kantor [4], of three-weight codes and few weights codes given by Ding [6], and Tonchev and Jungnickel [7]. We determine the optimal parameters of additive quaternary codes of short length.

References

[1] Arrieta, Eddie A., and Janwa, Heeralal.: A Go-Up Code Construction from Linear Codes Yielding Additive Codes for Quantum Stabilizer Codes. Proceedings of the $52nd$ Southeastern International Conference on Combinatorics, Graph Theory, and Computing, PROMS.

[2] Bonisoli, Arrigo.: Every Equidistant Linear Code is a Sequence of dual Hamming Codes. Ars Combinatoria. 18: $181 - 186$, 1983.

[3] Borges, Joaquim and Rifa, Josep and Zinoviev, Victor A.: On q-ary Linear Completely Regular Codes with $\rho = 2$ and Antipodal dual.

[4] Calderbank, Robert and Kantor, William M.: The Geometry of Two-Weight Codes. Bulletin of the London Mathematical Society. $18(2)$: $97 - 122$, 1986.

[5] Ding, Cunsheng and Luo, Jinquan and Niederreiter, Harald.: Two-weight Codes Punctured from Irreducible Cyclic Codes. Coding And Cryptology, World Scientific. pp $119 - 124$, 2008.

[6] Ding, Kelan and Ding, Cunsheng.: A Class of Two-Weight and Three-Weight Codes and Their Applications in Secret Sharing. IEEE Transactions on Information Theory. $61(11)$: $5835 - 5842$, 2015.

[7] Crnkovic, Dean and Svob, Andrea and Tonchev, Vladimir D.: Cyclotomic Trace Codes. Algorithms. $12(8)$, 2019.

[8] Assmus Jr, E.F and Mattson, Harold F.: Error-correcting codes: An axiomatic approach. Information and Control. $6(4)$: $315 - 330$, 1963.

[9] W. Wesley Peterson and E. J. Weldon, Jr.: ERROR-CORRECTING CODES. The Massachusetts Institute of Technology. 1972.

[10] Jungnickel, Dieter and Tonchev, Vladimir D.: On Bonisolis theorem and the block codes of Steiner triple systems. Designs, Codes and Cryptography. $86(3)$: $449 - 462$, 2018.

[11] Huffman, W Cary and Pless, Vera.: Fundamentals of Error-Correcting Codes. Cambridge university press. 2010.

[12] Ward, Harold N.: An Introduction to Divisible Codes. Designs, Codes and Cryptography. $17(1)$: $73 - 79$, 1999.

Construction of Entangled Assisted Quantum Error Correcting Codes from Monomial-Cartesian codes

Ramakrishna Bandi[1]***, Sanjit Bhowmick***[2]***, Satya Bagchi***[2]
`[ramakrishna@iiitnr.edu.in, sanjitbhowmick392@gmail.com, satya.bagchi@maths.nitdgp.ac.in]`

[1] Department of Mathematics
International Institute of Technology Naya Raipur
Nava Raipur - 493661, India
[2] Department of Mathematics
National Institute of Technology Durgapur
Durgapur, India

A monomial-Cartesian code is evaluated through monomials on Cartesian sets. It is a generalization of toric codes, affine Cartesian codes and J-affine variety codes, etc. In this talk, we discuss monomial-Cartesian codes. First compute the minimum distance of a monomial-Cartesian code and then determine the dual of monomial-Cartesian code using the tools of linear algebra. later, using duality, we give a necessary and sufficient condition on an LCD, self-orthogonal and self-dual codes. As an application, we consider a class of Quantum codes called Entanglement Assisted Quantum Qrror Correcting Code (EAQECC)s. Here we first prove that an EAQECC is maximum distance seperable (MDS) if and only if the corresponding linear code is MDS. This leads to the construction of MDS EAQECCs to MDS codes with l dimensional Hulls. We later show that there exists an MDS code of dimension k with l dimensional Hull, $0 \leq l \leq k$. Finally, we present some MDS EAQECCs with the minimum distance better than the EAQECCs available in the literature for a given entangled state c.

Construction and Linearity of Some $\mathbb{Z}_{p^s}$-Linear Generalized Hadamard Codes[*]

Dipak K. Bhunia* , *Cristina Fernández-Córdoba, Mercè Villanueva
[{Dipak.Bhunia,Cristina.Fernandez,Merce.Villanueva}@uab.cat]

Department of Information and Communications Engineering
Universitat Autònoma de Barcelona
08193 Cerdanyola del Vallès, Spain

Let $\mathbb{Z}_{p^s}$ be the ring of integers modulo p^s with $s \geq 1$ and p prime. The set of n-tuples over $\mathbb{Z}_{p^s}$ is denoted by $\mathbb{Z}_{p^s}^n$. A code over $\mathbb{Z}_p$ of length n is a nonempty subset of $\mathbb{Z}_p^n$, and it is linear if it is a subspace of $\mathbb{Z}_p^n$. Similarly, a nonempty subset of $\mathbb{Z}_{p^s}^n$ is a $\mathbb{Z}_{p^s}$-additive if it is a subgroup of $\mathbb{Z}_{p^s}^n$. Note that, when $p = 2$ and $s = 1$, a $\mathbb{Z}_{p^s}$-additive code is a binary linear code and, when $p = 2$ and $s = 2$, it is a quaternary linear code or a linear code over $\mathbb{Z}_4$.

In [5], a Gray map from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ is defined as $\phi(0) = (0, 0)$, $\phi(1) = (0, 1)$, $\phi(2) = (1, 1)$ and $\phi(3) = (1, 0)$. There exist different generalizations of this Gray map, which go from $\mathbb{Z}_{p^s}$ to

$\mathbb{Z}_p^{p^{s-1}}$ [2, 3, 6, 7]. The one given in [2] is the map $\phi : \mathbb{Z}_{p^s} \rightarrow \mathbb{Z}_p^{p^{s-1}}$ defined as follows:

$$\phi(u) = (u_{s-1}, \dots, u_{s-1}) + (u_0, \dots, u_{s-2})Y, \tag{1}$$

where $u \in \mathbb{Z}_{p^s}$, $[u_0, u_1, \dots, u_{s-1}]_p$ is the p-ary expansion of u, that is, $u = \sum_{i=0}^{s-1} p^i u_i$, and Y is a matrix of size $(s-1) \times p^{s-1}$ which columns are the elements of $\mathbb{Z}_p^{s-1}$.

Then, we define $\Phi : \mathbb{Z}_{p^s}^n \rightarrow \mathbb{Z}_p^{np^{s-1}}$ as the component-wise Gray map ϕ.

Let $\mathcal{C}$ be a $\mathbb{Z}_{p^s}$-additive code of length n. We say that its image $C = \Phi(\mathcal{C})$ is a $\mathbb{Z}_{p^s}$-linear code of length $p^{s-1}n$. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_{p^s}^n$, it is isomorphic to an abelian structure $\mathbb{Z}_{p^s}^{t_1} \times \mathbb{Z}_{p^{s-1}}^{t_2} \times \cdots \times \mathbb{Z}_{p^2}^{t_{s-1}} \times \mathbb{Z}_p^{t_s}$, and we say that $\mathcal{C}$, or equivalently $C = \Phi(\mathcal{C})$, is of type $(n; t_1, \dots, t_s)$. Note that $|\mathcal{C}| = p^{st_1} p^{(s-1)t_2} \cdots p^{t_s}$.

A generalized Hadamard (GH) matrix $H(p, \lambda) = (h_{ij})$ of order $n = p\lambda$ over $\mathbb{Z}_p$ is a $p\lambda \times p\lambda$ matrix with entries from $\mathbb{Z}_p$ with the property that for every i, j, $1 \leq i < j \leq p\lambda$, each of the multisets $\{h_{is} - h_{js} : 1 \leq s \leq p\lambda\}$ contains every element of $\mathbb{Z}_p$ exactly λ times [11].

An ordinary Hadamard matrix of order 4μ corresponds to a GH matrix $H(2, \lambda)$ over $\mathbb{Z}_2$, where $\lambda = 2\mu$ [1]. Two GH matrices of order n are said to be equivalent if one can be obtained from the other by a permutation of the rows and columns and adding the same element of $\mathbb{Z}_p$ to all the coordinates in a row or in a column. We can always change the first row and column of a GH matrix into zeros and we obtain an equivalent GH matrix which is called normalized. From a normalized Hadamard matrix H, we denote by F_H the code over $\mathbb{Z}_p$ consisting of the rows of H, and C_H the one defined as $C_H = \bigcup_{\alpha \in \mathbb{F}_q} (F_H + \alpha\mathbf{1})$, where $F_H + \alpha\mathbf{1} = \{\mathbf{h} + \alpha\mathbf{1} : \mathbf{h} \in F_H\}$ and $\mathbf{1}$ denotes the all-one vector. The code C_H over $\mathbb{Z}_p$ is

[*] This work has been partially supported by the Spanish MINECO under Grant PID2019-104664GB-I00 / AEI / 10.13039/501100011033.

called generalized Hadamard (GH) code [10]. Note that C_H is generally nonlinear over $\mathbb{Z}_p$. The $\mathbb{Z}_{p^s}$-additive codes that, under the Gray map Φ, give a GH code are called $\mathbb{Z}_{p^s}$-additive GH codes and the corresponding Gray map images are called $\mathbb{Z}_{p^s}$-linear GH codes.

The linearity of $\mathbb{Z}_4$-linear Hadamard codes of length 2^t was proved in [8, 9]. Later, in [4], an iterative construction for $\mathbb{Z}_{2^s}$-linear Hadamard codes was described, and the linearity of these codes was established. In this paper, we generalize these results for $\mathbb{Z}_{p^s}$-linear GH codes. Specifically, first, we show some results related to the Carlet's generalized Gray map. Then, we describe an iterative construction to obtain $\mathbb{Z}_{p^s}$-additive GH codes of type $(n; t_1, \dots, t_s)$. Finally, we show for which types the corresponding $\mathbb{Z}_{p^s}$-linear codes are nonlinear codes over $\mathbb{Z}_p$ when $p \neq 2$.

References

[1] E. F. Assmus; J. D. Key, Designs and Their Codes, Cambridge University Press, Great Britain, 1992.

[2] C. Carlet, *$\mathbb{Z}_{2^k}$-linear codes*, IEEE Trans. Inform. Theory, 44, no. 4, pp. 1543–1547, 1998.

[3] S. T. Dougherty; C. Fernández-Córdoba, *Codes over $\mathbb{Z}_{2^k}$, Gray map and self-dual codes*, Advances in Mathematics of Communications, 5, no. 4, pp. 571–588, 2011.

[4] C. Fernández-Córdoba; C. Vela; M. Villanueva, *On $\mathbb{Z}_{2^s}$-linear Hadamard codes: kernel and partial classification*, Designs, Codes and Cryptography, vol. 87, no. 2-3, pp. 417–435, 2019.

[5] A. R. Hammons; P. V. Kumar; A. R. Calderbank; N. J. A. Sloane; P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory, 40, no. 2, pp. 301–319, 1994.

[6] A. A. Nechaev; T. Khonol'd, *Weighted modules and representations of codes*, Probl. Inf. Transm., 35, no. 3, pp. 205–223, 1999.

[7] D. S. Krotov, *On $\mathbb{Z}_{2^k}$-dual binary codes*, IEEE Trans. Inform. Theory, 53, no 4, pp. 1532–1537, 2007.

[8] D. S. Krotov, *$\mathbb{Z}_4$-linear Hadamard and extended perfect codes*, International Workshop on Coding and Cryptography, ser. Electron. Notes Discrete Math. 6, pp. 107–112, 2001.

[9] K. T. Phelps; J. Rifà; M. Villanueva, *On the additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes: rank and kernel*, IEEE Trans. Inform. Theory, 52, no. 1, pp. 316–319, 2006.

[10] S. T. Dougherty; J. Rifà; M. Villanueva, *Ranks and kernels of codes from generalized Hadamard matrices*, IEEE Trans. Inform. Theory, 62, no. 2, pp. 687–694, 2016.

[11] D. Jungnickel, *On difference matrices, resolvable transversal designs and generalized Hadamard matrices*, Math. Zeitschrift, vol. 167, no. 1, pp. 49-60, 1979.

A software program for equivalence of linear codes over finite fields[†]

Iliya Bouyukliev, Stefka Bouyuklieva [{iliyab,stefka}@math.bas.bg]

Faculty of Mathematics and Informatics
St. Cyril and St. Methodius University of Veliko Tarnovo
Veliko Tarnovo, Bulgaria

The equivalence test is a main part in any classification problem. In this talk, we present the algorithm for equivalence of linear codes over finite fields implemented in the program LCEQUIVALENCE which is a module of the software package QEXTNEWEDITION [1]. The program is designed to obtain the inequivalent codes in a set of linear codes over a finite field $\mathbb{F}_q$ with $q \leq 64$ elements. Moreover, the program calculates the orders of the automorphism groups and orbits of the coordinates. The use does not require special programming language skills. Although there are many classification results, software for equivalence of linear codes is presented only in the works of J. Leon [6], Thomas Feulner [4] and Iliya Bouyukliev [2] (up to our knowledge). The main advantages of the program LCEQUIVALENCE are: (1) it works for codes over fields with $q \leq 64$ elements; (2) it can be used to find the inequivalent among a huge number of linear codes; (3) there is no restrictions on the length and dimension of the considered codes (this depends only on the used hardware and the computational time).

The main idea in the algorithm is not new - we associate with each code a $\{0,1\}$ matrix such that two codes are equivalent if and only if the corresponding binary matrices are isomorphic. A similar idea was used in [2] - the code equivalence problem was reduced to an isomorphism test of binary matrices. The problem in [2] is that not every automorphism of the binary matrix used is an automorphism of the code and therefore additional verification is needed. The authors of [3] proposed to use a different binary matrix as an image of a given q-ary code to avoid the disadvantage of [2]. A new improvement is implemented in the program LCEQUIVALENCE.

Let $\mathbb{F}_q^n$ be the n-dimensional vector space over the finite field $\mathbb{F}_q$. The *Hamming distance* between two vectors of $\mathbb{F}_q^n$ is defined as the number of coordinates in which they differ. A *q-ary linear $[n,k,d]_q$ code* is a k-dimensional linear subspace of $\mathbb{F}_q^n$ with minimum distance d. A *generator matrix* G of a linear code $[n,k]$ code C is any matrix of rank k (over $\mathbb{F}_q$) with rows from C. The most important definitions in our work are the following.

Definition 1: We say that two linear $[n,k]_q$ codes C_1 and C_2 are **equivalent**, if the codewords of C_2 can be obtained from the codewords of C_1 via a finite sequence of transformations of the following types: (1) permutation of coordinate positions; (2) multiplication of the elements in a given position by a non-zero element of $\mathbb{F}_q$; (3) application of a field automorphism to the elements in all coordinate positions.

This definition is well motivated as the transformations (1)–(3) preserve the Hamming distance and the linearity (for more details see [5, Chapter 7.3]). An *automorphism* of a linear code C is a finite sequence of transformations of type (1)–(3), which maps each codeword of

[†] This work is supported in part by the Bulgarian National Science Fund under Contracts KP-06- Russia/33/17.12.2020 and KP-06-N32/2-2019.

C onto a codeword of C. The set of automorphisms of C forms a group which is called the *automorphism group* of the code and denoted by $\mathrm{Aut}(C)$. Clearly, $\mathrm{Aut}(C)$ is the semidirect product of a group of monomial matrices by a subgroup of the Galois group of the considered finite field.

Definition 2: Two binary matrices of the same size are **isomorphic** if the rows of the second one can be obtained from the rows of the first one by a permutation of the columns.

Any permutation of the columns of a binary matrix A which maps the rows of A into the rows of the same matrix, is called an automorphism of A. The set of all automorphisms of A is a subgroup of the symmetric group S_n and we denote it by $\mathrm{Aut}(A)$.

Let C be a linear code over the field $\mathbb{F}_q$ with $q = p^m$ elements, where p is a prime, and let α be a primitive element of $\mathbb{F}_q$. To any element of $\mathbb{F}_q$ we juxtapose a circulant binary matrix of order $q-1$ in the following way:

$$0 \mapsto \mathrm{circ}(00\ldots0), \quad \alpha^i \mapsto \mathrm{circ}(0\ldots0\underbrace{1}_{i}0\ldots0) \text{ for } i = 0, 1, \ldots, q-2.$$

Instead of a generator matrix, we use a generating set D_C for the code C. This is a set of codewords that is stable under the action of the group $\mathrm{Aut}(C)$ and generates the code as a linear space over $\mathbb{F}_q$. Obviously, if $v \in D_C$ then $\alpha^i v \in D_C$ for $i = 0, \ldots, q-2$. Therefore we take a subset $D'_C \subset D_C$ such that any two vectors in D'_C are nonproportional and any vector from D_C is proportional to a vector in D'_C. We substitute any vector $v = (v_1, v_2, \ldots, v_n) \in D'_C$ with a binary $(q-1) \times 2n(q-1)$ matrix in the following way: first, we extend v to $v' = (0, v_1, 0, v_2, \ldots, 0, v_n) \in \mathbb{F}_q^{2n}$ and then we replace each coordinate of v' by its corresponding circulant matrix. In this way we correspond to the set D'_C a binary $t(q-1) \times 2n(q-1)$ matrix A'_C, where $t = |D'_C|$. We then add a few more rows in order to restrict the automorphisms of the binary matrix to those permutations that correspond to the automorphisms of the linear code.

The basic features of the program LCEQUIVALENCE are presented on the website [1]. A more detailed description will be given in the talk.

References

[1] I. Bouyukliev, *QextNewEdition - LCequivalence module* (2021). Online available at http://www.moi.math.bas.bg/moiuser/~data/Software/QextNewEditionLCequiv.html.

[2] I. Bouyukliev, *About the code equivalence*, in *Advances in Coding Theory and Cryptology*, T. Shaska, W. Huffman, D. Joyner, and V. Ustimenko, Eds., pp. 126–151, 2007.

[3] I. Bouyukliev; M. Dzhumalieva-Stoeva, *Representing equivalence problems for combinatorial objects*, Serdica J. Computing **8**(4), 327–354 (2014)

[4] T. Feulner, *The automorphism groups of linear codes and canonical representatives of their semilinear isometry classes*, Advances in Mathematics of Communication **3**(4), 363-383 (2009)

[5] P. Kaski; P. R. J. Östergård, *Classification Algorithms for Codes and Designs*, Springer-Verlag Berlin Heidelberg, 2006.

[6] J. Leon, Computing automorphism groups of error-correcting codes, IEEE Transactions on Information Theory **28**, 496–511 (1982)

Recent conjectures on the equivalence of linear cyclic codes

Reza Dastbasteh*, *Petr Lisoněk [{rdastbas,plisonek}@sfu.ca]

Department of Mathematics,
Simon Fraser University
Burnaby, Canada

In this work, three recent conjectures on the equivalence of linear cyclic codes over finite fields will be answered. These conjectures were recently proposed by Aydin et al. (2019) based on their computational results on the parameters of linear cyclic codes. In particular, we prove the following statements.

1. If $g_1(x)$ and $g_2(x)$ are the generator polynomials of two monomially equivalent linear cyclic codes of length n over $\mathbb{F}_q$, then $g_1(x)$ and $g_2(x)$ generate two monomially equivalent linear cyclic codes of length nm, provided that $\gcd(mn, q) = 1$.
2. Let A_1 and A_2 be the defining sets of two linear cyclic codes of length n over $\mathbb{F}_q$. If the shift map $\phi(x) = (x + b) \mod n$ is a bijection from A_1 to A_2, then the linear cyclic codes with the defining sets A_1 and A_2 are monomially equivalent and $n \mid |A_1|(q-1)b$.
3. We show that there are monomially equivalent linear cyclic codes that are not equivalent by an affine map.

Most of our results were motivated by computer algebra experiments. As an application, several infinite families of monomially equivalent linear cyclic codes are provided.

References

[1] N. Aydin; J. Lambrinos; O. VandenBerg, *On equivalence of cyclic codes, generalization of a quasi-twisted search algorithm, and new linear codes*, Designs, Codes and Cryptography, 2019 Oct 1;87(10):2199-212.

[2] K. Bogart; D. Goldberg; J. Gordon, *An elementary proof of the MacWilliams theorem on equivalence of codes*, Information and Control, 1978 Apr 1;37(1):19-22.

[3] PP. Palfy, *Isomorphism problem for relational structures with a cyclic automorphism. European Journal of Combinatorics*, 1987 Jan 1;8(1):35-43.

[4] F.J. MacWilliams; N.J.A. Sloane, *The theory of error-correcting codes*, Elsevier.

Hulls of additive conju-cyclic codes over F4 with respect to a trace dual

Md Ajaharul Hossain[1] ***, Ramakrishna Bandi***[1]***, Sanjit Bhowmick***[2]***,***
[{mdajaharul,ramakrishna}@iiitnr.edu.in,
sanjitbhowmick392@gmail.com]

[1] Department of Mathematics
International Institute of Technology Naya Raipur
Nava Raipur - 493661, India
[2] Department of Mathematics
National Institute of Technology Durgapur
Durgapur, India

Conjucyclic codes are closed under the conjugate cyclic shift operations. Additive Conjucyclic codes are useful in quantum error-correction, for which this class of codes are new topic of interest in algebraic coding theory. In this talk, we discuss additive conjucyclic codes over $\mathbb{F}_4$ with respect to the trace dual and obtain conditions for an additive conjucyclic code to be self-orthogonal and self-dual. Later we find the trace hull of an additive conjucyclic code and its dimension. A necessary and sufficient condition for a conjucyclic code to have an additive complementary dual (ACD) is obtained. Finally, a condition on additive conjucyclic complementary pair of codes over $\mathbb{F}_4$ is found using trace dual. We end the talk by presenting some good quantum codes constructing using the conjucyclic codes.

Quantum Error-Correcting Codes over small fields from AG curves

Heeralal Janwa, Fernando Piñero [{heeralal.janwa,fernando.pinero1}@upr.edu]

Department of Mathematics
University of Puerto Rico at Rio Piedras
17 University Ave. Ste 1701 San Juan PR, 00925-2537

In this article we use hyperbolic codes from algebraic curves over high degree extensions of $\mathbb{F}_2$ to construct self–orthogonal code pairs for Quatum Error Correcting codes. We also present bounds on the parameters of the resulting subfield codes over $\mathbb{F}_2$ or $\mathbb{F}_4$ from Hermitian curves, Norm–Trace curves, quasi–Hermitian curves, and others. Several of these results are novel and provide a pathway to make progress towards making quantum computers feasible and practical during the next decade.

References

[1] Hernando, Fernando; McGuire, Gary, *Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions*, Journal of Algebra, 2011

[2] Férard, Eric, *A infinite class of Kasami functions that are not APN infinitely often*, Contemp. Math., Vol. 686, pag. 45–63, 2017

[3] Delgado, Moises; Janwa, Heeralal, *Some new results on the conjecture on exceptional APN functions and absolutely irreducible polynomials: the Gold case*, Advances in Mathematics of Communications, 2017

[4] Delgado, Moises; Janwa, Heeralal, *On the absolute irreducibility of hyperplane sections of generalized Fermat varieties in $\mathbb{P}^3$ and the conjecture on exceptional APN functions: the Kasami-Welch degree case*, 2016

[5] Aubry, Yves; McGuire, Gary; Rodier, François, *A few more functions that are not APN infinitely often*, Finite fields: theory and applications, Amer. Math. Soc., Providence, RI, 2010

Skew constacyclic codes over a non-chain ring

Mehmet E. Köroğlu **,** ***Mustafa Sarı***
[{mkoroglu,musari}@yildiz.edu.tr]

Department of Mathematics
Yildiz Technical University
Esenler 34220, Istanbul-Turkey

A subspace of the vector space $\mathbb{F}_q^n$ with dimension k is called a linear code of length n and dimension k over $\mathbb{F}_q$. The elements of a linear code are termed as codewords. The minimum Hamming distance d of a linear code $\mathcal{C}$ is the minimum Hamming weight $w_H(\mathcal{C})$ of $\mathcal{C}$, where $w_H(\mathcal{C}) = \min\{w_H(c) : 0 \neq c \in \mathcal{C}\}$ and $w_H(c) = |\{i : c_i \neq 0,\, i \in \{0,1,\ldots,n-1\}\}|$. A linear code $\mathcal{C}$ over $\mathbb{F}_q$ of length n, dimension k and minimum distance d is denoted by the triple $[n,k,d]_q$ and this code corrects up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors. An $[n,k,d]_q$ linear code is called maximum distance separable (MDS) if $k = n - d + 1$. A linear code $\mathcal{C}$ over $\mathbb{F}_q$ is called a linear complementary dual (LCD) code if $Hull(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^{\perp} = \{\mathbf{0}\}$, where $\mathcal{C}^{\perp} = \left\{ y \in \mathbb{F}_q^n : \sum_{i=0}^{n-1} x_i y_i = 0,\, \forall x \in \mathcal{C} \right\}$.

For a given automorphism θ of $\mathbb{F}_q$, the set

$$\mathbb{F}_q[x;\theta] = \{a_0 + a_1 x + \ldots + a_1 x^n | a_i \in \mathbb{F}_q \text{ and } n \in \mathbb{N}\}$$

of formal polynomials forms a ring under the usual addition of polynomials and the polynomial multiplication with the restriction $xb = \theta(b)x$. The multiplication is extended to all the elements of $\mathbb{F}_q[x;\theta]$ via distributivity and associativity. This ring is called the *skew polynomial ring* over $\mathbb{F}_q$.

For a given element $\lambda \in \mathbb{F}_q - \{0\}$ and an automorphism θ of $\mathbb{F}_q$ a skew λ-constacyclic code over the finite field $\mathbb{F}_q$ of length n is a linear code $\mathcal{C}$ satisfying that

$$(\lambda\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in \mathcal{C}$$

for each codeword $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in \mathcal{C}$.

In the last few decades, codes over finite commutative chain rings were studied extensively (see Refs. [1, 2, 3, 4, 5, 6]). In recent years, some special non-chain rings have been used as an alphabet for codes (see Refs. [7, 8, 9, 10]). One important class of linear codes is the class of constacyclic codes since their algebraic structure and their applications to other disciplines including classical and quantum communication systems. Over the conventional polynomial rings, the algebraic structure of λ-constacyclic codes of length n is determined by the factors of the cyclotomic polynomial $x^n - \lambda$. In [11], Boucher, Solé and Ulmer used skew polynomials to describe the structure of constacyclic codes under a skew constacyclic shift. Later, in the [12, 13, 14], Boucher and Ulmer investigated more properties and good examples of these codes.

In this study, we examine the algebraic structure of the semi-local ring $\mathcal{R}_q = \mathbb{F}_q[v]/\langle v^2+1\rangle$, where $q = p^k$ is a prime power and for positive integers a and b, $p = a^2 + b^2$, and determine the automorphisms of this ring to study the algebraic structure of the skew constacyclic codes and their dual over this ring. We provide the necessary and sufficient conditions for the existence of the self-dual and self orthogonal skew constacyclic codes. In addition, we give the conditions for the existence of the linear complementary dual skew cyclic codes and skew negacyclic codes.

References

[1] M.C.V. Amarra; F.R. Nemenzo, *On* $(1-u)$*-cyclic codes over* $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$, Appl. Math. Letters, **21**, 1129-1133 (2008).

[2] A. Bonnecaze; P. Udaya, *Cyclic codes and self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory, **45**(4), 1250-1255 (1999).

[3] H.Q. Dinh; S. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory, **50**(8), 1728-1744 (2004).

[4] S. Jitman; S. Ling; P. Udomkavanich, *Skew constacyclic codes over finite chain rings*, Adv. Math. Commun., **6**(1), 39-63 (2012).

[5] E. Martínez-Moro; I.F. Rúa, *Multivariable codes over finite chain rings: serial codes*, SIAM J. Discrete Math., **20**(4), 947-959 (2006).

[6] G.H. Norton; A. Sâlâgean, *Strong Gröbner bases and cyclic codes over a finite-chain ring*, Electron. Notes Discrete Math., **6**, 240-250 (2001).

[7] J. Gao; F. Ma; F. Fu, *Skew constacyclic codes over the ring* $\mathbb{F}_q + v\mathbb{F}_q$, Appl. Comput. Math, **6**(3), 286-295 (2017).

[8] J. Gao, *Skew cyclic codes over* $\mathbb{F}_q + v\mathbb{F}_q$, J Appl Math Informatics, **31**(3-4), 337-342 (2013).

[9] F. Gursoy; I. Siap; B. Yildiz, *Construction of skew cyclic codes over* $\mathbb{F}_q + v\mathbb{F}_q$, Adv. Math. Commun., **8**(3), 313-322 (2014).

[10] M. Shi; T. Yao; P. Solé, *Skew cyclic codes over a non-chain ring*, Chin. J. Electron., **26**(3), 544-547 (2017).

[11] D. Boucher; P. Solé; F. Ulmer, *Skew constacyclic codes over Galois rings*, Adv. Math. Commun., **2**(3), 273-292 (2008).

[12] D. Boucher; F. Ulmer, *Codes as modules over skew polynomial rings*, Lecture Notes Comput. Sci., **5291**, 38-55 (2009).

[13] D. Boucher; F. Ulmer, *Coding with skew polynomial rings*, J. Symbolic Comput., **44**(12), 1644-1656 (2009).

[14] D. Boucher; F. Ulmer, *Self-dual skew codes and factorization of skew polynomials*, J. Symbolic Comput., **60** 47-61 (2014).

$\mathbb{F}_q\mathcal{R}$-Skew Cyclic Codes

Shikha Patel*, *Om Prakash [{shikha_1821ma05,om}@iitp.ac.in]

Department of Mathematics
Indian Institute of Technology Patna
Bihta, Patna - 801 106, India

Let p be a prime and $\mathbb{F}_q$ be a finite field of order $q = p^m$. In this paper, we study skew cyclic codes over $\mathbb{F}_q\mathcal{R}$ where $\mathcal{R} := \mathbb{F}_q + u\mathbb{F}_q$ with $u^2 = u$. To characterize $\mathbb{F}_q\mathcal{R}$-skew cyclic codes, first we establish the algebraic structure and then by considering an inner product the self-orthogonality of these codes are discussed. Further, we construct a Gray map over $\mathbb{F}_q\mathcal{R}$ and discuss the Gray images of $\mathbb{F}_q\mathcal{R}$-skew cyclic codes over $\mathbb{F}_q$. Finally, we provide various examples of skew cyclic codes over $\mathbb{F}_q\mathcal{R}$ and their respective Gray images for different lengths.

Keywords
Cyclic code, Skew cyclic code, Self-orthogonal code, Gray map.

A New Algorithm on Finite Fields for the Construction of Differentially 4-Uniform Permutations with Optimal Algebraic Degree[‡]

Roberto Reyes Carranza[1], ***Heeralal Janwa***[2]
`[{roberto.reyes,heeralal.janwa}@upr.edu]`

[1] College of Business
University of Puerto Rico at Mayaguez
Mayaguez PR 00682, USA
[2] Department of Mathematics
University of Puerto Rico at Rio Piedras
17 University Ave. Ste 1701 San Juan PR, 00925-2537

The Advanced Encryption Standard uses the inverse function, which is a differential 4-uniform function. Finding differential 4-uniform permutations with high nonlinearity on even degree field extensions is a current big challenge. In [1], Bracken and Leander listed that as an open problem (only a few results are know). It is known that if *f* is an permutation on F_{2^n}, then $\deg(f) \leq n-1$. If *f* attains the equality Zha [2] calls it optimal algebraic degree function. To know more about a class of sporadic binomials permutations with low differential uniformity ($\delta = 4$, 6), see the work of Charpin and Kyureghyan (2017) in [3]. Yu and Wang built differential 6 and 4-uniform permutations from the inverse function [5]. Then Qu et al. [4] gives us a survey of differentially 4-uniform permutation families, even without the requirement of high nonlinearity (see Carlet [6], and Zha [2]).

We construct new families of δ-uniform permutations in even degree field extensions (also for odd degree extensions), where δ can be $4, 6, 8$. It is important to underline that the functions given by almost all authors are defined implicitly, or are given as a piecewise function. While our functions are given via an explicit formula in polynomial representation, which is the more desired representation. In this process, we obtain a new general and practical theorem that can be widely applied in any finite field, e.g., to new S-Boxes.

References

[1] Carl Bracken; Gregor Leander, *A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree*, *Finite Fields Appl.*, 16(4):231–242, 2010.

[2] Zhengbang Zha; Lei Hu; Siwei Sun, *Constructing new differentially 4-uniform permutations from the inverse function*, *Finite Fields Appl.*, 25:64–78, 2014.

[3] Pascale Charpin; Gohar M. Kyureghyan, *On sets determining the differential spectrum of mappings*, *Int. J. Inf. Coding Theory*, 4(2-3):170–184, 2017.

[‡] The research of Roberto Carlos Reyes Carranza was partially supported by the NSF. The research of Heeralal Janwa was supported by NASA. Some of the computations were carried out at the High Performance Computing Center of UPR.

[4] Longjiang Qu; Yin Tan; Chik How Tan; Chao Li, *Constructing differentially 4-uniform permutations over $F_{2^{2k}}$ via the switching method*, *IEEE Trans. Inform. Theory*, 59(7):4675–4686, 2013.

[5] Yuyin Yu; Mingsheng Wang; Yongqiang Li, *Constructing differentially 4 uniform permutations from known ones*, *Chinese Journal of Electronics*, 22(3):495–499, 2013.

[6] Claude Carlet, *On known and new differentially uniform functions*, *Australasian Conference on Information Security and Privacy*, pages 1–15. Springer, 2011.

Enumeration and Construction of New Boolean Bent/Near-bent Functions of the Gold and Kasami-Welch Type[§]

Jose W. Velazquez, Heeralal Janwa [{jose.velazquez16,heeralal.janwa}@upr.edu]

Department of Mathematics
University of Puerto Rico at Rio Piedras
17 University Ave. Ste 1701 San Juan PR, 00925-2537

A vectorial (m,k) Boolean function is defined as $f : F_{2^m} \to F_{2^k}, 1 \leq k \leq m$. Boolean functions ($k = 1$) have their nonlinearity bounded above by $2^{m-1} - 2^{\frac{m}{2}-1}$. Bent Boolean functions have maximum nonlinearity; a measure of their distance to the set of affine functions (i.e., the first-order Reed-Muller codes). Janwa and Wilson gave construction of error-correcting-codes [4] from non-linear function. Janwa, McGuire and Wilson [3] conjectured that such codes are 2-error-correcting if and only if the exponents are the Gold or Kasami-Welch type ($d = 2^l + 1, 2^{2l} - 2^l + 1, (l, m) = 1$) (i.e., the functions are APN). One can can construct Boolean functions as trace functions on F_{2^m}. Well known Boolean functions are the Gold and Kasami-Welch near-bent functions of the form $Tr(x^d)$ [1]. Corresponding to these exponents, Dillon and Dobbertin [2] proposed a construction of bent functions of the type $Tr(\lambda x^d)$ with $\lambda \in F_{2^m}^*$ a non-cube. In this work, we generalize the results of Dillon and Dobbertin. We also give results on the classification and enumeration of the Gold and Kasami-Welch near-bent functions via cyclotomic coset equivalence analysis. Consequently, we prove theorems and obtain bounds on the number of equivalence classes of such near-bent functions. We also prove some such results for the bent functions of Dillon and Dobbertin and of our generalization.

References

[1] C. Carlet and S. Mesnager. Four decades of research on bent functions. *Designs, Codes and Cryptography*, 78(1):5–50, 2016.

[2] J. Dillon and H. Dobbertin. New cyclic difference sets with singer parameters. *Finite Fields and Their Applications*, 10(3):342–389, 2004.

[§] This research is funded by the PR Space Grant Consortium, NASA Cooperative Agreement 80NSSC20M0052

[3] H. Janwa, G. Mcguire, and R. M. Wilson. Double-error-correcting cyclic codes and absolutely irreducible polynomials over gf (2). *Journal of Algebra*, 178(2):665–676, 1995.

[4] H. Janwa and R. M. Wilson. Hyperplane sections of fermat varieties in p3 in char. 2 and some applications to cyclic codes. In G. Cohen, T. Mora, and O. Moreno, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 180–194, Berlin, Heidelberg, 1993. Springer Berlin Heidelberg.

Some Constructions of l-Galois LCD codes

Shikha Yadav, Om Prakash [{1821ma10,om}@iitp.ac.in]

Department of Mathematics
Indian Institute of Technology Patna
Bihta, Patna - 801 106, India

Let F_q be the finite field with q elements, where $q = p^m$ for some prime p and $m > 0$. In this article, we provide three constructions of linear codes over F_q in terms of their generator matrices and characterise LCD codes from them. Here, we consider Galois inner product instead of Euclidean or Hermitian inner products. For these constructions, we use the matrices A for which $A[\sigma^{m-l}(A)]^t = I, 0 \leq l \leq m-1$, where σ is the frobenius map.

S8. Computer Algebra for Geometry and Combinatorics

Organized by

Anton Betten and Fatma Karaoglu

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

Classifying Cubic Surfaces and Associated Objects

Anton Betten[1] [Anton.Betten@colostate.edu]

[1] Department of Mathematics, Colorado State University, Fort Collins, CO 8526, USA

Classification means determining the possible isomorphism types of a class of objects under the action of the symmetry group of the space in which the objects are considered. Classification is different from separation by invariants, which is weaker, as nonisomorphic objects may have the same set of invariants. One example is the problem of classifying cubic surfaces in three dimensional projective space over some field $\mathbb{F}$. The goal of classification is to provide all possible examples that can exist. This is helpful in the study of the properties of the objects, and it can provide insight into how the objects arise and how they are related. Classification is often hard, and computers can be used to support the work. This is especially true if the field $\mathbb{F}$ is assumed to be finite.

The talk will survey ongoing work with **Alice Hui**, **Nathan Kaplan** and **Fatma Karaoglu** regarding the classification of cubic surfaces and their associated structures such as quartic curves, Schläfli double sixes, general sets of points in a plane called arcs. Computer algebra comes in as an application of group theory to the problem of computing orbits. The groups are matrix groups over finite fields. The orbit algorithms are often based on partially ordered sets, in order to build the structures step-by-step.

What does this approach give? We can produce specific new examples of objects. We can produce computer-free theorems about the objects, for instance their symmety groups. This helps deepen previous knowledge that provided coarser information about the objects that was not at the level of classification up to isomorphism but separation by various geometric invariants such as the number of Eckardt points or the number of lines on the surface. Work over finite fields can be meaningful for algebraic objects in characteristic zero, as the example of the Eckardt surface shows, which was recently rediscovered over finite fields of odd characteristic.

Keywords
Cubic Surface, Projective Geometry, Quartic Curve, Arc, Computer Algebra

Construction of transitive q-designs

Dean Crnković[1]***, Vedrana Mikulić Crnković***[1]***, Andrea Švob***[1] [deanc@math.uniri.hr]

[1] Department of Mathematics, University of Rijeka, Rijeka, Croatia

The notion of q-analog of designs has been introduced by Delsarte [2]. In 1987, Thomas [4] constructed the first non-trivial q-analog of design with parameters 2-$(n, 3, 7; 2)$, $n > 6, n = 6k + 1$ or $n = 6k - 1$. An important result was given in [1], where the authors constructed a design over a finite field with parameters 2-$(13, 3, 1; 2)$ which was the first known example of a Steiner q-design that does not arise from spreads. In this talk we will present a method of constructing transitive q-designs, which is a generalization of the method for constructing transitive designs given in [2].

Keywords
block design, q-design, transitive group

References

[1] M.Braun, T. Etzion, P. Östergård, A. Vardy, A. Wassermann, Existence of q-analogs of Steiner systems. *Forum of Math Pi* **4**, e7, 14 pages (2016).
[2] D. Crnković, V. Mikulić Crnković, A. Švob, On some transitive combinatorial structures constructed from the unitary group $U(3, 3)$. *J. Statist. Plann. Inference* **144**, 19–40 (2014).
[3] P. Delsarte, Association schemes and t-designs in regular semilattices. *J. Comb. Theory Ser. A* **20**, 230–243 (1976).
[4] S. Thomas, Designs over finite fields. *Geomet. Dedic.* **24**, 237–242 (1987).

On (locally Hermitian) ovoids of $H(3, q^2)$

Bart De Bruyn[1] [Bart.DeBruyn@UGent.be]

[1] Department of Mathematics: Algebra and Geometry, Ghent University, Ghent, Belgium

The points and lines of $\mathrm{PG}(3, q^2)$ that are totally isotropic with respect to a given Hermitian polarity of $\mathrm{PG}(3, q^2)$ define a generalized quadrangle which we denote by $H(3, q^2)$. An *ovoid* O of $H(3, q^2)$ is a set of points meeting each line in a *singleton*. Such an ovoid is called *locally Hermitian* if there exists a point x on $H(3, q^2)$ and q^2 lines $L_1, L_2, \ldots, L_{q^2}$ of $\mathrm{PG}(3, q^2)$ through x such that $O = (L_1 \cup L_2 \cup \cdots \cup L_{q^2}) \cap H(3, q^2)$. There exists a connection between locally Hermitian ovoids of $H(3, q^2)$ and so-called indicator sets of the affine plane $\mathrm{AG}(2, q^2)$ [3].

In my talk, I will discuss several new results about (locally Hermitian) ovoids of $H(3, q^2)$ [2]. This includes among others a complete classification of all ovoids of $H(3, 9)$. The results have been obtained or have been inspired by computer computations using a Computer Algebra System.

Keywords
(Locally Hermitian) ovoid, (Hermitian) generalized quadrangle, indicator set

References

[1] A. E. Brouwer; H. A. Wilbrink, *Ovoids and fans in the generalized quadrangle Q(4,2)*. Geom. Dedicata 36 (1990), 121–124.

[2] B. De Bruyn, *On ovoids of the generalized quadrangle* $H(3, q^2)$. Ann. Comb. 25 (2021), 495–514.

[3] E. Shult, *Problems by the wayside*. Discrete Math. 294 (2005), 175–201.

Disjoint sets in projective planes

Mustafa Gezek[1] [mgezek@nku.edu.tr]

[1] Department of Mathematics, Tekirdağ Namık Kemal University, Tekirdağ, Turkey

Point sets in projective planes with two-line intersections have been studied in finite geometry a lot. Maximal arcs and unitals are examples of such sets. For example, in the known projective planes of order 16, 36 maximal $(52, 4)$-arcs and 156 unitals are known to exist [1-5]. It was pointed out that vt-sets of type $((t-1)k, tk)$ might arise from the unions of t pairwise disjoint maximal (v, k)-arcs [3]. In this talk, we discuss the results of a number of computer searches related to maximal arcs and unitals in some of the projective planes. Previous to our work, all known 104-sets of type $(4, 8)$ associated with maximal arcs of degree 4 were coming from isomorphic copies of maximal $(52, 4)$-arcs [4]. Our computations show that such sets exist from non-isomorphic pairs as well [1]. Two different methods for finding v-sets of type (a, b) are discussed.

Keywords
Prjoective plane, Maximal arc, Unital

References

[1] M. GEZEK, *Combinatorial problems related to codes, designs and finite geometries*. PhD thesis, Michigan Technological University, 2017.
[2] M. GEZEK, R. MATHON, V.D. TONCHEV, Maximal arcs, codes, and new links between projective planes of order 16. *The Electronic Journal of Combinatorics* **27**(1), P1.62 (2020).
[3] N. HAMILTON, *Maximal arcs in finite projective planes and associated in projective planes*. PhD thesis, The University of Western Australia, 1995.
[4] N. HAMILTON, S.D. STOICHEV, V.D. TONCHEV, Maximal arcs and disjoint maximal arcs in projective planes of order 16. *Journal of Geometry* **67**(1-2), 117-126 (2000).
[5] S.D. STOICHEV, M. GEZEK, Unitals in projective planes of order 16. *Turkish Journal of Mathematics* **45**(2), 1001-1014 (2021).

The usage of Maple in solving Schrödinger's wave equation for an optical atom model

Latif A-M. Hanna[1], *Shoukry S. Hassan*[2] [latif.hanna@ku.edu.kw]

[1] Department of Mathematics, Kuwait University, Kuwait
[2] Department of Mathematics, Bahrain University, Kingdom of Bahrain

Steinberg in [1,2], introduced a method for solving certain types of partial differential equations. The method is based on the use of the Lie algebraic decomposition techniques, which exploits a faithful matrix representation of least degree of the Lie algebra. The method was applied to many models in quantum optics.

Recently, in [3], the method was used to solve the Schrödinger's wave equation of the two-level optical atom model. Faithful matrix representation of this model, and others, were assisted by the Maple packages. Maple also, was very useful in utilizing the solution of the wave function for presenting the graphs of the atomic localization in the coordinate space. Generalizations of the model in [3], to the q-deformed Lie algebra of possible faithful matrix representations [4] is outlined.

Keywords
Lie algebra, faithful representation, Schrödinger's wave equation, optical atom model.

References

[1] S. STEINBERG, Applications of the Lie algebraic formulas of Baker, Campbell, Hausdorff, and Zassenhaus to the calculation of explicit solutions of partial differential equations. *J. Differential Equations* **26**(3), 404-434 (1997).
[2] S. STEINBERG, Lie series, Lie transformations, and their applications, *Lie Methods in Optics,* J.S. Mondragón and K.B. Wolf, (eds.), *Lecture Notes in Phys.*, Springer (**250)** 45-103, (León, 1985), 1986.
[3] LATIF HANNA, RANIA ALHARBEY, SEBAWE ABDALLA AND SHOUKRY HASSAN, Algebraic Method of Solution of Schrödinger's Equation of a Quantum Model. *WSEAS Transactions on Mathematics* **19**(43), 421-429 (2020).
[4] L. A-M. HANNA, On faithful matrix representations of q-deformed Lie algebra for coupled quantized oscillators. *International Journal of Applied Mathematics (IJAM)* **33**(6), first 1083-1098 (2020).

Counting Arcs in the Projective Plane

Nathan Kaplan[1] [nckaplan@math.uci.edu]

[1] Department of Mathematics, University of California, Irvine, CA, USA

How many collections of n points in the projective plane over a finite field of size q have no 3 on a line? For $n \leq 6$, the formula is a polynomial in q [1]. For $7 \leq n \leq 9$, the formula is quasipolynomial [1,2,3]. For example, when $n = 7$ there is one polynomial formula that holds for odd q and a different one for even q. In this talk we will discuss the case $n = 10$ where the formula involves the number of $\mathbb{F}_q$-points on certain elliptic curves and K3 surfaces and is no longer quasipolynomial. We will emphasize computational and algorithmic aspects of this problem and will mention connections to coding theory. We will explain difficulties in adapting these ideas to deal with larger n. This is joint work with Isham, Weinreich, Lawrence, Kimport and Peilen.

Keywords
Arcs, projective planes, MDS codes.

References

[1] D. GLYNN, *Rings of geometries. II.* J. Combin. Theory Ser. A 49 (1988), no. 1, 26-66.
[2] A. IAMPOLSKAIA; A. N. SKOROBOGATOV; E. SOROKIN, *Formula for the number of* $[9, 3]$ *MDS codes*. IEEE Trans. Inform. Theory 41 (1995), no. 6, 1667-1671.
[3] N. KAPLAN; S. KIMPORT; R. LAWRENCE; L. PEILEN; M. WEINREICH, *Counting arcs in the projective plane via Glynn's algorithm*. J. Geom. 108 (2017), no. 3, 1013-1029.

Cubic Surfaces with 27 Lines and 13 Eckardt Points

Fatma Karaoglu[1,2]***, Anton Betten***[1] [fkaraoglu@nku.edu.tr]

[1] Department of Mathematics, Colorado State University, Fort Collins, CO 8526, USA
[2] Department of Mathematics, Tekirdag Namik Kemal University, Tekirdag, Turkey

A cubic surface is an algebraic variety of degree three in projective three space. Important geometric invariants are the number of lines on the cubic surface and the number of Eckardt points, which are points where three lines of the surface are concurrent. In this talk, we focus on cubic surfaces with 27 lines and 13 or 45 Eckardt points. Two cubic surface with same number of lines and the same number of Eckardt points may be projectively distinct.

We classify the cubic surfaces with 27 lines over a field of even characteristic with 13 or 45 Eckardt points. We give a concise description of all cubic surfaces with these properties and compute the automorphism groups of them. This work generalizes earlier work by Hirschfeld [4] which settles the case of 45 Eckardt points.

This work is based on the relation between cubic surfaces with 27 lines and 6-arcs in a plane [2], on the configuration of Eckardt points [3] and the automorphism groups of 6-arcs. Furthermore, the tables of cubic surfaces over small finite fields from [1] are used.

Keywords
Finite Geometry, Grup Theory, Eckardt Points, Configurations

References

[1] A. BETTEN AND F. KARAOGLU, Cubic surfaces over small finite fields. *Des. Codes Cryptogr.* **87**(4), 931–953 (2019).
[2] F.E. ECKARDT, Ueber diejenigen Fl¨achen dritten Grades, auf denen sich drei gerade Linien in einem Punkte schneiden. *Math. Ann.* **10**, 227–272 (1876).
[3] J. W. P. HIRSCHFELD, Classical configurations over finite fields. I. The double- six and the cubic surface with 27 lines. *Rend. Mat. e Appl.* **26**(5), 115–152 (1967).
[4] J. W. P. HIRSCHFELD, The double-six of lines over PG(3, 4). *J. Austral. Math. Soc.* **4**, 83–89 (1964).

Betti Numbers of Numerical Semigroup Rings

Pınar Mete[1] [pinarm@balikesir.edu.tr]

[1] Department of Mathematics, Balıkesir University, Balıkesir, Turkey

Minimal free resolution of a finitely generated k-algebra is an important source to extract information about the algebra. Therefore, finding an explicit minimal free resolution of a standard k-algebra is one of the main problems in commutative algebra and algebraic geometry. Even it is not always easy to obtain a description of the differential in the resolution, we can still get some information about the numerical invariants of the resolution such as Betti numbers.

A numerical semigroup is a subsemigroup of the nonnegative integers that has a finite complement. Numerical semigroups appear in various branches of mathematics ranging from singularity theory to number theory. There is a close relationship between monomial curves and numerical semigroups. This close relation allows us to use the algebraic geometry terminology in studying numerical semigroups.

In this talk, we will give brief and recent results related to the Betti numbers of numerical semigroup rings and of their tangent cones [1],[2],[3].

Keywords
Numerical Semigroup Rings, Tangent Cones, Betti Numbers, Monomial Curves

References

[1] P. METE, On the Betti numbers of the tangent cones for Gorenstein monomial curves. Preprint, arXiv:2105.04012 [math.AC]
[2] P. METE, EE. ZENGIN, Minimal free resolutions of the tangent cones for Gorenstein monomial curves. *Turkish Journal of Math.* **43** 2782-2793 (2019).
[3] DI. STAMATE, Betti numbers for numerical semigroup rings. *Multigraded Algebra and Applications*, **238** 133-157, Springer Proceedings in Mathematics and Statistics, Springer, Cham 2018.

Parameters of Affine Hermitian Grassmann Codes

Fernando Piñero González[1]***, Doel Rivera Laboy***[2] [fernando.pinero1@upr.edu]

[1] Department of Mathematics, University of Puerto Rico in Ponce, Ponce PR.
[2] Department of Mathematics, Pontificial Catholic University of Puerto Rico, Ponce, PR.

Abstract

The Grassmannian is arguably one of the most widely studied objects in Algebraic Geometry. The Grassmannian is embedded into projective space via the Plücker embedding. One of the techniques most often employed is to make a linear code from the projective points. This code is known as the Grassmann code. Nogin [1] determined the parameters of the Grassmann code for general field size q. The Grassmannian also has special subvarieties known as polar Grassmannians. A polar Grassmannian is a subvariety of the Grassmannian defined-only by subspaces isotropic under a bilinear or sesquilinar form. In case this form is Hermitian, it is known as the polar Hermitian Grassmannian. Cardinali and Guizzi determined the parameters of the polar Hermitian Grassmann code for 2–dimensional spaces. In this work we consider Affine Hermitian Grassmann codes. These codes may be considered as the linear codes defined from one of the affine maps of the polar Hermitian Grassmannian. We also consider these as evaluation codes. We determine their length, dimension and minimum distance. Affine Hermitian Grassmann codes also improve on the minimum distance os Affine Grassmann codes for similar parameters.

1 Introduction

The Grassmannian $(\mathcal{G}_{\ell,m})$ is the collection of all vector spaces of dimension ℓ of a vector space V of length m. We take $V = \mathbb{F}_q^m$. This is a highly interesting and well studied geometry with a rich algebraic structure.

It is well known that the Grassmannian may be embedded into a projective space through the Plücker embedding. In order to study the properties of the Grassmannian we make use of a linear code.

2 Preliminaries

Let q be a prime power, we let $\mathbb{F}_q$ denote the finite field of q elements.

Definition 1. *If M is a square matrix, then the minor $M^{I,J}$ is the determinant of the submatrix of M obtained from the rows I and columns J.*

Definition 2. *A matrix M over $\mathbb{F}_{q^2}$ is hermitian if $M_{j,i} = M_{i,j}^q$. We denote the collection of $\ell \times \ell$ Hermitian matrices over $\mathbb{F}_{q^2}$ by $\mathbb{H}^\ell(\mathbb{F}_{q^2})$.*

2.1 Affine Hermitian Grassman Code

For $\ell \geq 1$ we denote $X = [X_{ij}]$ as an $\ell \times \ell$ matrix of indeterminates where X_{ij}.

Definition 3. $\Delta(\ell)$ *is the set of all minors of the matrix X. That is:*

$$\Delta(\ell) := \{det_{I,J}(X^{I,J}), I, J \subseteq [\ell], |I| = |J|\}$$

Definition 4. *We define* $\mathcal{F}(\ell)$ *as the subspace of* $\mathbb{F}_{q^2}$*–linear combinations of elements of* $\Delta(\ell)$.

$$\mathcal{F}(\ell) := \{ \sum_{I,J \subseteq [\ell], \# I = \# J} f_{I,J} det_{I,J}(X^{I,J}), f_{I,J} \in \mathbb{F}_{q^2} \}$$

Definition 5. *The evaluation map of* $\mathbb{F}_{q^2}[X]$ *is the map*

$$Ev\text{: } \mathbb{F}_{q^2}[X] \rightarrow \mathbb{F}^n_{q^2} \text{ defined by } Ev(f) := (f(P_1), ..., f(P_n)).$$

Lemma 1.

$$\dim C^{\mathbb{H}}(\ell) = \binom{2\ell}{\ell}.$$

Theorem 2. *Suppose that* $\ell \geq 2$. *Then the minimum distance of the code* $C^{\mathbb{H}}(\ell)$ *is* $q^{\ell^2} - q^{\ell^2-1} - q^{\ell^2-3}$.

In the next two sections of the paper we work out a proof by induction of this fact. Our proofs will use the elementary techniques of polynomial evaluation and bounding the number of zeroes with the degree of a polynomial to determine the minimum distance of $C^{\mathbb{H}}(\ell)$.

References

[1] D.Yu. Nogin, *Codes associated to Grassmannians*, in: R. Pellikaan, M. Perret, S.G. Vladut (Eds.), Arithmetic Geometry and Coding Theory (Luminy, 1993), Walter de Gruyter, Berlin/New York, 1996, pp. 145–154.

[2] I. Cardinali and L. Giuzzi, Line Hermitian Grassmann codes and their parameters *Finite Fields and their Applications* **51** May 2018, 407–432.

[3] P. Beelen, S. Ghodepade and T. Høholdt,Affine Grassmann codes *IEEE Trans. on Info. Theory* **56**(7), 3166–3176. (2010)

Algebraic Invariants of Codes on Weighted Projective Spaces

***Yağmur Çakıroğlu* [1], *Mesut Şahin*[1]** [mesut.sahin@hacettepe.edu.tr]

[1] Mathematics Department, Hacettepe University, Ankara, Turkey

Weighted projective spaces are natural generalizations of classical projective spaces having rich structures and exhibiting interesting algebraic geometric properties. They have been regarded in literature, see [1-3], as convenient ambient spaces to create interesting classes of linear codes over finite fields.

The purpose of this talk is to introduce these codes known as *Weighted Projective Reed–Muller codes* over a finite field, and to reveal the role of computer algebra packages to study some of the relevant combinatorial commutative algebraic invariants. We pay a particular attention on two dimensional case to obtain more explicit information about the *minimal free resolution* of the vanishing ideal of the weighted projective plane $\mathbb{P}(1, a, b)$ over $\mathbb{F}_q$. This yields to the Hilbert function giving the dimension of the code and regularity index which is crucial to eliminate trivial codes.

Keywords
linear codes, weighted projective space, free resolution, Hilbert function

References

[1] Y. AUBRY, W. CASTRYCK, S. R. GHORPADE, G. LACHAUD, M. E. O'SULLIVAN, AND S. RAM., Hypersurfaces in weighted projective spaces over finite fields with applications to coding theory. In *Algebraic Geometry for Coding Theory and Cryptography*, E. Howe, K. Lauter and J. Walker (eds.), 25–61, Springer, 2017.

[2] O. GEIL; C. THOMSEN, Weighted Reed–Muller codes revisited.*Des. Codes Cryptogr.* 66 **volume**(66), 195–220. (2013).

[3] A. B. SORENSEN, Weighted Reed–Muller codes and algebraic-geometric codes. *IEEE Trans.Inf.Theory* **volume**(38), 1821–1826. (1992).

Quasi-symmetric 2-$(41, 9, 9)$ designs and doubly even self-dual codes of length 40

Akihiro Munemasa[1], *Vladimir D. Tonchev*[2] [tonchev@mtu.edu]

[1] Graduate School of Information Sciences, Tohoku University, Sendai, Japan
[2] Mathematics Department, Michigan Technological University, Houghton, Michigan, U.S.A.

The residual design of a quasi-symmetric 2-$(41, 9, 9)$ design with block intersection numbers 1 and 3 is a quasi-symmetric 1-$(40, 8, 9)$ design with block intersection numbers 0 and 2. The incidence matrix of the latter generates a binary doubly even code of length 40. Using the database of binary doubly even self-dual codes of length 40 classified by Betsumiya, Harada and Munemasa [1], we prove that a quasi-symmetric 1-$(40, 8, 9)$ design with block intersection numbers 0 and 2 is not extendable to a quasi-symmetric 2-$(41, 9, 9)$ design with block intersection numbers 1 and 3, provided that it has a fixed-point-free automorphism of order 5 and 2-rank 20. This may be considered as a first step to prove the nonexistence of a quasi-symmetric 2-$(41, 9, 9)$ design with block intersection numbers 1 and 3, and an analogue of the previous work [2], [3] for quasi-symmetric 2-$(37, 9, 8)$ designs with block intersection numbers 1 and 3.

Keywords
quasi-symmetric design, binary code

References

[1] K. Betsumiya, M. Harada and A. Munemasa, A complete classification of doubly even self-dual codes of length 40. *Electronic J. Combin.* **19**, #P18 (12 pp.) (2012).
[2] S. Bouyuklieva and Z. Varbanov, Quasi-symmetric 2-$(37, 9, 8)$ designs and self-orthogonal codes with automorphisms of order 5, *Math Balkanica (N.S.)* **19**, 33–38 (2005).
[3] M. Harada, A. Munemasa and V.D. Tonchev, Self-dual codes and the nonexistence of a quasi-symmetric 2-$(37, 9, 8)$ design with intersection numbers 1 and 3. *J. Combin. Des.* **25**(10), 469–476 (2017).

Towards the classification of unitals on 28 points of low rank

***Vladimir Tonchev*[1], *Alfred Wassermann*[2]** [alfred.wassermann@uni-bayreuth.de]

[1] Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931, USA
[2] Department of Mathematics, University of Bayreuth, 95440 Bayreuth, Germany

Unitals are combinatorial 2-$(q^3 + 1, q + 1, 1)$ designs. The classical examples are the *Hermitian unital* $H(q)$, defined by the absolute points and absolute lines of a unitary polarity in the desarguesian plane of order q^2 and for $q = 3^{2m+1}$ the *Ree unital* $R(q)$, invariant under the Ree group. However, already for the case $q = 3$, a complete classification is missing. In 1981, Brouwer [2] constructed for $q = 3$ more than 130 further nonisomorphic unitals, i.e. 2-$(28, 4, 1)$ designs. He observed that the 2-rank of the constructed unitals is at least 19. Here, the p-rank of a design is defined as the rank of the incidence matrix between points and blocks of the design over the finite field GF(p). In 1998, McGuire, Tonchev and Ward [4] proved that indeed the 2-rank of a unital on 28 points is between 19 and 27 and that the Ree unital is the unique 2-$(28, 4, 1)$ design of 2-rank 19. In the same year, Jaffe and Tonchev [3] showed that there is no unital on 28 points of 2-rank 20 and there are exactly 4 isomorphism classes of unitals of rank 21.

Here, we present the complete classification by computer of unitals of 2-rank 22, 23 and 24. There are 12 isomorphism classes of unitals of 2-rank 22, 78 isomorphism classes of unitals of 2-rank 23, and 298 isomorphism classes of unitals of 2-rank 24.

Keywords
Combinatorial designs, finite geometry, combinatorial enumeration

References

[1] A. BETTEN, D. BETTEN, V. TONCHEV, *Unitals and codes.* Discrete Mathematics **267** 23–33 (2003).

[2] A. E. BROUWER, Some unitals on 28 points and their embedding in projective planes of order 9. In *Geometry and Groups*, Lecture Notes in Mathematics **893**, 183–188. M. Aigner, D. Jungnickel (eds.), Springer Berlin, (1981).

[3] D. B. JAFFE, V. TONCHEV, *Computing linear codes and unitals.* Designs, Codes and Cryptography **14** 39–52 (1998).

[4] G. MCGUIRE, V. TONCHEV, H. N. WARD, *Characterizing the Hermitian and Ree unitals on 28 points.* Designs, Codes and Cryptography **13** 57–61 (1998).

Parallelisms of $PG(3,4)$ invariant under noncyclic automorphism groups of order 4

Anton Betten[1]***, Svetlana Topalova***[2]***, Stela Zhelezova***[2] [stela@math.bas.bg]

[1] Colorado State University, USA
[2] Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Bulgaria

$\mathrm{PG}(n,q)$ denotes the n-dimensional projective space over $GF(q)$. A spread in $\mathrm{PG}(n,q)$ is a set of lines such that each point is in exactly one line. A parallelism is a partition of the lines of the projective space to spreads [3,4]. Spreads and parallelisms have interesting relations and multiple applications. General constructions are known for $\mathrm{PG}(n,2)$, $\mathrm{PG}(2^n-1,q)$ and $\mathrm{PG}(3,q)$. All parallelisms of $\mathrm{PG}(3,2)$ and $\mathrm{PG}(3,3)$ are known [1]. Their classification in larger projective spaces is presently infeasible and only smaller classes are usually concerned.

$\mathrm{PG}(3,4)$ is the smallest projective space in which parallelisms have not yet been classified. The parallelisms with nontrivial automorphisms of odd prime orders have already been constructed [5]. There exist, however, plenty of parallelisms with automorphisms of order 2 and their classification is a challenging problem. Parallelisms with cyclic automorphism groups of order 4 have been constructed too [2]. In the present paper we classify the parallelisms invariant under noncyclic groups of order 4. As a result, all the parallelisms of $\mathrm{PG}(3,4)$ which possess automorphism groups of order greater than 2 are already known. The problem of the classification of parallelisms with full automorphism groups of order at most 2 remains open.

Keywords
Projective space, parallelism, automorphism, combinatorial design.

References

[1] A. BETTEN, The packings of $\mathrm{PG}(3,3)$. *Des. Codes Cryptogr.* **79** (3), 583–595 (2016).
[2] A. BETTEN; S. TOPALOVA; S. ZHELEZOVA, Parallelisms of $\mathrm{PG}(3,4)$ invariant under cyclic groups of order 4. In *Algebraic Informatics. CAI 2019. Lecture Notes in Computer Science, vol. 11545*, Ćirić M., Droste M., Pin JÉ. (eds), 88–99, Springer, Cham (2019).
[3] N. L. JOHNSON, *Combinatorics of Spreads and Parallelisms.* Series: Chapman & Hall Pure and Applied Mathematics, CRC Press (2010).
[4] L. STORME, Finite Geometry. In *Handbook of Combinatorial Designs*, Colbourn, C., Dinitz, J. (eds.), *Discrete mathematics and its applications*, Rosen, K. (eds.) 702–729. CRC Press, Boca Raton, FL. (2007).
[5] S. TOPALOVA; S. ZHELEZOVA, New parallelisms of $PG(3,4)$. *Electronic Notes in Discrete Mathematics* **57**, 193–198 (2017).

How do we construct new maximum rank distance codes?

Ferdinando Zullo[1] [ferdinando.zullo@unicampania.it]

[1] Dipartimento di Matematica e Fisica, Università degli Studi della Campania "Luigi Vanvitelli", Caserta, Italy

The set $\mathbb{F}_q^{m\times n}$ of $m \times n$ matrices over $\mathbb{F}_q$ is a metric space with rank metric distance defined by $d(A,B) = \mathrm{rk}(A-B)$ for $A, B \in \mathbb{F}_q^{m\times n}$. A subset $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ is called *rank metric code*.

These codes were introduced independently by Delsarte [3] and Gabidulin [4]. They also proved a Singleton-like bound for these codes which involves the parameters of the code. If this bound is achieved, then $\mathcal{C}$ is called a *maximum rank distance code*, or shortly *MRD-code*. Such codes have received great attention in recent years for their applications in cryptography and coding theory.

For many years only few different new constructions of MRD codes have been discussed. In 2016 twisted Gabidulin codes have been introduced by Sheekey, and then generalized by Lunardon, Trombetti and Zhou. Remarkably, in his paper Sheekey pointed out a connection between 2-dimensional $\mathbb{F}_{q^n}$-linear MRD codes and scattered linear sets of maximum rank in $\mathrm{PG}(1, q^n)$.

In this talk we will consider 2-dimensional $\mathbb{F}_{q^n}$-linear MRD codes and we will see how *Computer Algebra* plays an important role in this area, such as it can be used

- to find first some examples of MRD codes for fixed values of the parameters;
- to prove that certain rank metric codes are MRD codes.

This is based on the papers [1,2,5,6,7].

Keywords
Rank metric code, Linear set, MRD code

References

[1] D. Bartoli, C. Zanella and F. Zullo, A new family of maximum scattered linear sets in $\mathrm{PG}(1, q^6)$. *Ars Mathematica Contemporanea* **19**(1), 125–145 (2020).
[2] B. Csajbók, G. Marino and F. Zullo, New maximum scattered linear sets of the projective line. *Finite Fields and Their Applications* **54**, 133–150 (2018).
[3] P. Delsarte, Bilinear forms over a finite field, with applications to coding theory. *Journal Combinatoria Theory Series A* **25**(3), 226-241 (1978).
[4] E. Gabidulin, Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii* **21**(1), 3–16 (1985).
[5] G. Marino, M. Montanucci and F. Zullo, MRD-codes arising from the trinomial $x^q + x^{q^3} + cx^{q^5} \in \mathbb{F}_{q^6}[x]$. *Linear Algebra and its Applications* **591**, 99–114 (2020).
[6] A. Neri, P. Santonastaso and F. Zullo, Extending two families of maximum rank distance codes. *arxiv preprint*.

[7] C. ZANELLA AND F. ZULLO, Vertex properties of maximum scattered linear sets of $\mathrm{PG}(1, q^n)$. *Discrete Mathematics* **343**(5), 111800 (2020).

S10. Polytopes - Algebra - Computation (PAC)

Organized by

Gizem Sungu and Zafeirakis Zafeirakopoulos

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

Normaliz meets Lawrence: polytope volume by signed decomposition

Winfried Bruns [wbruns@uos.de]

Universität Osnabrück, Institut für Mathematik, 49069 Osnabrück, Germany

Since 2001 Normaliz has computed polytope volumes, and meanwhile it has three main algorithms. The most recent (version 3.9.0, July 2, 2021, https://github.com/Normaliz/Normaliz/releases) is the Lawrence algorithm that computes polytope volumes via signed decomposition.

A driving challenge has been applications to social choice (see [1], [2]) where we had already reached elections with four candidates that define polytopes of dimension 23. Five candidates elections and, thus, polytopes of dimension 119 were behind the horizon. They have now been reached.

The Lawrence algorithm uses that a “generic” triangulation of the dual induces a signed decomposition of the primal polytope. Let the full dimensional polytope P be represented as the intersection of a pointed cone $C \subset \mathbb{R}^d$ and a hyperplane defined by a “grading”, i.e., a linear form $\gamma \in (\mathbb{R}^d)^*$, as $H = \{x : \gamma(x) = 1\}$. A triangulation Δ of the dual cone C^* is generic if γ is not contained in any hyperplane G intersecting a simplicial cone δ of Δ in a facet. This implies that γ is contained in the interior of exactly one of the chambers, say in D_δ, into which $(\mathbb{R}^d)^*$ is subdivided by the hyperplanes G through the facets of δ. This implies that $D_\delta^* \cap H$ is a (bounded) polytope $Q_\delta \subset H$. The collection of the Q_δ is a signed decomposition of P. In terms of volumes,

$$\operatorname{vol} P = \sum_\delta (-1)^{e_\delta} \operatorname{vol} Q_\delta$$

where e_δ counts the number of hyperplanes G through facets of δ with $\gamma \in G^-$, $\delta \subset G^+$. See [4] or, for a proof in our language, [3].

In applications the polytope P is often defined by a small number of inequalities relative to its dimension. Then the dual cone C^* has few extreme rays, and therefore C^* has a “small” triangulation. But there is a snag: the only known way to find a generic triangulation chooses Δ by taking a “ generic” vector g in C^* and then all pyramids with apex in g and basis in a “hollow” triangulation of the boundary of C^*.

The computation proceeds in four stages:

1. Find a triangulation Δ_0 of C^*.
2. Find the hollow triangulation induced by Δ_0.
3. Find a generic point.
4. Compute the volume.

To reach our goal for the applications to social choice, we had to be able to cope with $\dim C = 120$ and 128 inequalities. In this order of magnitude all four steps need a sophisticated implementation. Fortunately Normaliz has been able to master step (1) for many years. Step (2), which is more difficult as one might think, unfortunately increases the size of the triangulation. Step (3) is the main source of evil: g inevitably has large coordinates. As a consequence, the polytopes Q_δ above have complicated rational vertices. While it is not so difficult to compute each single volume, the addition of volumes can produce gigabyte filling fractions. For such cases Normaliz has a fixed precision mode that computes $\operatorname{vol} P$ within an easily found error bound. The default choice for the precision is 100 decimal digits. (The rational arithmetic of Normaliz is based on GMP.)

To give an impression of the order of magnitude let us mention the "Condorcet efficiency of plurality voting": $\dim C = 120$, 128 inequalities, $|\Delta_0| \approx 2.5 * 10^9$, $|\Delta| \approx 50 * 10^9$. For this computation a (still) fast machine tales about a week for steps (1)–(3) and ≈ 600 GB of RAM. The generic vector has entries of size $\approx 10^{10}$. On the same machine, step (4) would take several weeks, despite of shared memory parallelization . However, since the volumes of the simplices Q_δ can be computed independently of each other, one can distribute step (4) to the nodes in a high performance cluster. The Osnabrück HPC then does the work in < 12 hours.

Remark. Also vinci (https://www.math.u-bordeaux.fr/~aenge/) offers the Lawrence algorithm. However, vinci's floating point arithmetic cannot cope with the numerical intricacies of the Lawrence algorithm in high dimension. Normaliz uses only integer and rational arithmetic. Euclidean volumes are derived from lattice normalized volumes at the end.

Keywords
Polytope volume, Lawrence algorithm, social choice

References

[1] W. Bruns and B. Ichim, Polytope volume by descent in the face lattice and applications in social choice. *Math. Prog. Comp.* **113**, 415–442 (2020).
[2] W. Bruns, B. Ichim and C. Söger, Computations of volumes and Ehrhart series in four candidates elections. *Ann. Oper. Res.* **280**, 241–265 (2019).
[3] P. Filliman, The volume of duals and sections of polytopes. *Mathematika* **39**, 67–80 (1992)
[4] J. Lawrence, Polytope volume computation. *Math. Comp.* **57**, 259–271 (1991).

Tropical refinement

Carles Checa, National Kapodistrian University of Athens.

July 1, 2021

Abstract

In some problems of polytopes and computer algebra, it may be interesting to decide when a coherent mixed subdivision $S(\phi)$ of a setting of polytopes $\Delta = (\Delta_1, \dots, \Delta_r)$ refines another subdivision $S(\psi)$, meaning that all its cells are contained in some cell of the latter.
The normal fan of the mixed subdivision of $S(\psi)$, which is given by a tropcal curve which is the skeleton of a polyhedral complex may give us the answer.

In a recent publication of D'Andrea, Sombra and Jerónimo, where they give a proof of the Canny-Emiris rational formula for the sparse resultant, an interesting object appears as key. These are incremental chains of mixed subdivisions.

$$S(\theta_0) \preceq S(\theta_1) \preceq \cdots \preceq S(\theta_n)$$

where $S(\theta_i)$ is a mixed subdivision of $\Delta_0, \dots, \Delta_{i-1}, \sum_{j=i}^{n} \Delta_j$. For simplicity, they consider the lifting of this mixed subdivision on $\sum_{j=i}^{n} \Delta_j$ to be zero.
The condition of one subdivision refining another one is defined in the following way.

Definition 0.1. Let $S(\phi), S(\psi)$ be two mixed subdivisions of $\Delta = (\Delta_0, \dots, \Delta_n)$. We say that $S(\psi)$ refines $S(\phi)$ and write $S(\psi) \preceq S(\phi)$ if for every cell $C \in S(\psi)$ there is a cell $D \in S(\phi)$ such that $C \subset D$. We say that $S(\psi)$ mixedly refines $S(\psi)$ if, moreover, $C_i \subset D_i$ for all $i = 0, \dots, n$.

The question that follows is: if $S(\theta_i)$ is given, which conditions do we need to impose in the lifting of Δ_i in order to guarantee that $S(\theta_i) \preceq S(\theta_{i+1})$? The answer is given by the dual fans of these mixed subdivisions, which are tropical curves giving a polyhedral complex.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Polytopes - Algebra - Computation”*

Slack realization spaces and realizability of polytopes

***João Gouveia*[1], *Antonio Macchia*[2], *Amy Wiebe*[2]** [macchia@zedat.fu-berlin.de]

[1] Departamento de Matemática, Universidade de Coimbra, Coimbra, Portugal
[2] Department of Mathematics and Computer Science, Freie Universität Berlin, Berlin, Germany

The *slack realization space* is a recent model for the realization space of a polytope that represents each polytope by its slack matrix, the matrix obtained by evaluating its defining inequalities at each vertex [1, 2]. Unlike the classical model, the slack model naturally mods out projective transformations. It is inherently algebraic, arising as the positive part of a variety of a saturated determinantal ideal, and provides a new computational tool to study classical realizability problems.

We recently constructed a reduced slack model combining the slack variety with the more compact Grassmannian model [3]. This allows us to study cases that were previously out of computational reach. Using linear programming and the *SlackIdeals* package that we developed for *Macaulay2* [4], we establish for the first time the non-realizability of some large simplicial and quasi-simplicial spheres.

Keywords
Realization spaces, Slack matrices, Realizability of abstract polytopes

References

[1] J. GOUVEIA; A. MACCHIA; R. R. THOMAS; A. WIEBE, The slack realization space of a polytope. *SIAM J. Discrete Math.* **33** (3), 1637–1653 (2019).
[2] J. GOUVEIA; A. MACCHIA; R. R. THOMAS; A. WIEBE, Projectively unique polytopes and toric slack ideals. *J. Pure Appl. Algebra* **224** (5), paper 106229 (2020).
[3] J. GOUVEIA; A. MACCHIA; A. WIEBE, Combining realization space models of polytopes. *Preprint* (2020) [arXiv:2001.11999].
[4] A. MACCHIA; A. WIEBE, Slack Ideals in Macaulay2. In *Mathematical software – ICMS 2020*, A. Bigatti, J. Carette, J. Davenport, M. Joswig, T. de Wolff (eds.), 222–231. Lecture Notes in Computer Science, vol. **12097**, Springer, Cham, 2020.

A hidden variable model for universal quantum computation with magic states on qubits

Cihan Okay [cihan.okay@bilkent.edu.tr]

Bilkent University, Turkey

A central question in quantum information theory is to determine physical resources required for quantum computational speedup. In the model of quantum computation with magic states, classical simulation algorithms based on quasi-probability distributions, such as discrete Wigner functions, are used to study this question. For quantum systems of odd local dimension it has been known that negativity in the Wigner function can be seen as a computational resource. The case of qubits, however, resisted a similar approach for some time since the nice properties of Wigner functions for odd dimensional systems no longer hold for qubits. In our recent work we construct a hidden variable model, which replaces the Wigner function representation, for qubit systems where any quantum state can be represented by a probability distribution over a finite state space and quantum operations correspond to Bayesian update of the probability distribution. The state space is given by a polytope in the space of Hermitian matrices. The fundamental questions about quantum computational power is linked to the understanding of the vertices of this polytope. This is joint work with Michael Zurel and Robert Raussendorf; Phys. Rev. Lett. 125, 260404 (2020).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Polytopes - Algebra - Computation"*

Codes on Subgroups of Weighted Projective Torus

Mesut Şahin[1], ***Oğuz Yayla***[2] [mesut.sahin@hacettepe.edu.tr]

[1] Mathematics Department, Hacettepe University, Ankara, Turkey
[2] Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey

Toric varieties are interesting geometric objects lying on the crossroad of algebra, geometry and combinatorics. Their maximal torus is an algebraic group acting on the toric variety. To every lattice polytope there correspond to a projective toric variety and there is a dictionary between the two worlds of these polytopes and varieties. Many champion codes obtained from toric varieties appeared in the literature, see [1] for instance.

The simplest examples of toric varieties include classical and weighted projective spaces. Parameters of linear codes obtained by evaluating rational functions on a projective torus are computed in [4]. This idea is transferred to weighted projective tori and some parameters are computed in [2]. In both cases the vanishing ideal was a lattice ideal with a nice structure, which was shown to be true in general for subgroups in a toric variety [3].

The purpose of this talk is to introduce some linear codes on certain subgroups of the *weighted projective torus* over a finite field, and to share some formulas for their parameters in some cases. This will generalize the works in [2,4]. We also highlight the importance of computer algebra packages to study some of the relevant combinatorial and algebraic properties.

Keywords
toric codes, weighted projective tori, lattice ideals.

References

[1] G. BROWN; A. KASPRZYK, Seven new champion linear codes. *LMS J. Comput. Math.* **volume**(16), 109–117. (2013).

[2] E. DIAS; J. NEVES, Codes over a weighted torus. *Finite Fields and Their Appl.* **volume**(3), 66–79. (2015).

[3] M. ŞAHIN, Toric codes and lattice ideals. *Finite Fields Appl.* **volume**(52), 243–260. (2018).

[4] E. SARMIENTO; M. VAZ PINTO;R. H. VILLARREAL, The minimum distance of parameterised codes on projective tori. *Appl. Algebra Engrg. Comm. Comput.* **volume**(22), 249–264. (2011).

S11. Computer Algebra in Education

Organized by

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

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Computer Algebra in Education*

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

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

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

My first contact with computer algebra goes back to ***Derive*** in 1991. I will never forget what was written in the user manual introduction ([1]): «Making mathematics more exciting and enjoyable is the driving force behind the development of the ***Derive*** program. The system is designed to eliminate the drudgery of performing long tedious mathematical calculations. This gives you the freedom to explore different approaches to problems – approaches that you probably would not even consider if you had to do the calculations by hand ». And this also applies, at different levels, to many other computer programs (CAS but also DGS for instance).

Some textbooks contain many interesting exercises where use of CAS is recommanded but not mandatory. In [2], I don't often feel the "freedom to explore different approaches to problems" despite the fact that the book contains many exercises where the use of a computer is required. But in other cases (namely in [3]), heavy use of computer algebra makes a new way of teaching mathematics possible. Since many years, I have decided to add in my teaching some aspects not covered or not enough exploited by textbooks (this decision would have been difficult to take without the adoption of CAS technology all over the campus). But I have also decided to skip some "classical stuff": teachers should not forget the length of a semester is still the same! The talk will be about how CAS technology can be easily used to teach subjects where only pencil and paper techniques would discourage the user. Texas Instruments CAS software will be used for the computations. The first item in the following list will be used this year for the presentation. Future ACA conferences should be an occasion to select among the others.

- Computer algebra systems solving facilities can produce huge expressions users must be dealing with. Sometimes, the simplification of a formula can require a high level of manipulations. And this is where the teacher could act as a guide for the student. Here is an example: use a third degree polynomial equation where your students are asked to solve it using Newton's method. Then, take a look at the exact solution returned by a CAS and get the opportunity to use calculus, talk about Cardano's formula and trigonometric substitutions.

- Integral tables in calculus textbooks should be updated in order to benefit from more thant 30 years of computer algebra! Why not try to use a table where symetry among formulas becomes a goal whenever it is possible as the Rubi system does ([4])? A better choice of antiderivatives, the search for continuous antiderivatives and more explanations on the constant of integration should become new subjects instead of spending (too much) time on integration techniques.
- Real analysis and complex analysis don't seem to fit with computer algebra. But many concepts in (real and complex) analysis can be introduced and/or illustrated by CAS. Pointwise convergence of a series of functions, the Gibbs'phenomenom are examples. A built-in Laurent series function could be used to check the computation for a residue at a pole; the unwinding number could be used to verify some equalities involving logs and general powers as chapter of [5] ; 2D and 3D plotting facilities can be used for different transformations or to solve equations.

Some among us thought computer algebra systems were going to change the way we teach mathematics. It did but not as much as we would have expected. Blame for this whatever you want: the textbooks, the teachers, the students, the curriculum, the system. But things are not so bad: using CAS, many mathematics teachers have given themselves additional years of making "teaching more exciting and enjoyable". And the latter makes learning mathematics also exciting and enjoyable for many students.

Keywords
Computer algebra systems, textbooks.

References

[1] ***DERIVE*** *User Manual, version 2*. Fourth edition, Soft Warehouse, March 1991.

[2] STEWART, JAMES *Calculus, Concepts and Contexts*. 4e, Brooks/Cole, 2010.

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

[4] `https://rulebasedintegration.org/about.html`.

[5] ASLAKSEN, HELMER, *Can Your Computer Do Complex Analysis?*, in *Computer Algebra Systems: A Practical Guide*, 1st Edition, Edited by Michael J. Wester, 1999.

.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Session Title"*

A CAS-DGS assisted exploration of Spiric curves and their Hessians

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

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

During the last decades, several packages have been developed, both in Computer Algebra Systems (CAS) and in Dynamic Geometry Systems (DGS) for the study of plane algebraic curves. Using them, the study became experimental, involving graphics and animations, and algebraic computations. It involves exploration, discovery and then proof, all this based on a fruitful dialog between the kinds of software [4]. Even when the student does not master all the theoretical material, software may provide a bypass of the problem [1] and also incite to learn more mathematics.

We study here the points of inflexion of special biquartic curves called *spiric curves*, which appear as (b)isoptic curves of conics [2,3] . They can be realized as the intersection of a torus with a plane parallel to the torus's axis (recall that a torus is generated by revolving a circle around an axis). *Cassini ovals* are a special case of these spirics; they have been conjectured by the astronomer Cassini as a model for planetary motion. Kepler's law finally took the central place, and people claimed that these ovals lost their importance and became a pure geometric object. Actually, they still appear in various scientific domains, such as electrostatics, and isoptic curves. Generally in the literature, the revolving circle does not intersect the axis and a general form of the equation of the curve is

$$(x^2+y^2)^2 - 2a(x^2-y^2) + a^2 - b^2 = 0, \tag{1}$$

where a and b are positive real parameters.The limiting case where $a = 0$ is a (double) circle. In the situation described by Equation (1), the torus is a regular one, i.e. non self-intersecting:

1. If $a > b$, the curve is the union of two loops;
2. For $a = b$, the curve is a lemniscate;
3. If $a < b$, the curve is a single loop, which may have points of inflexions or not.

These cases reflect the distance from the center of the revolving circle to the axis; see Fig. 1.

In [4], offsets of these curves are explored and new constructions are shown. The needed dialog between a Computer Algebra System (CAS) and a Dynamic Geometry System (DGS) is analyzed there, in order to explore, conjecture and prove new results.

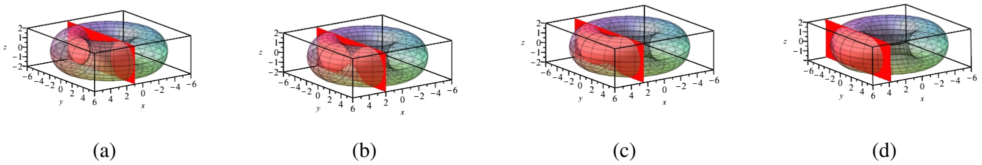

(a) (b) (c) (d)

Figure 1: Toric intersections

We work in a more general case, where the torus is self-intersecting, i.e. the revolving circle intersects the axis. These are the curves appearing as bisoptic curves of conics. In [1], the pair torus-plane is reconstructed from the data of the curve.

Depending on the distance from the center of the revolving circle to the rotation axis, the intersection may have either only one component, or two disjoint components. The distance center-axis influences also the existence of points of inflexion on the spiric. See Figure 1.

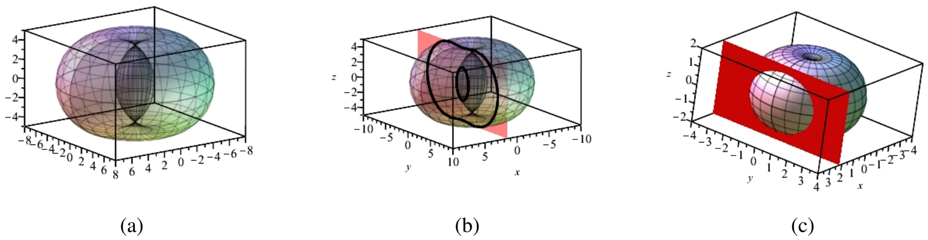

(a) (b) (c)

Figure 2: Plane intersection with a self-intersecting torus

The existence of points of inflexion is explored using the following theorem: for a given plane curve $\mathcal{C}$ given by an equation of the form $F(x,y)=0$, an associate curve is defined by the vanishing of the so-called *Hessian determinant*:

$$\begin{vmatrix} \frac{\partial^2}{\partial x^2}F(x,y) & \frac{\partial^2}{\partial x \partial y}F(x,y) \\ \frac{\partial^2}{\partial y \partial x}F(x,y) & \frac{\partial^2}{\partial x^2}F(x,y) \end{vmatrix}$$

We will call this curve the Hessian of $\mathcal{C}$.

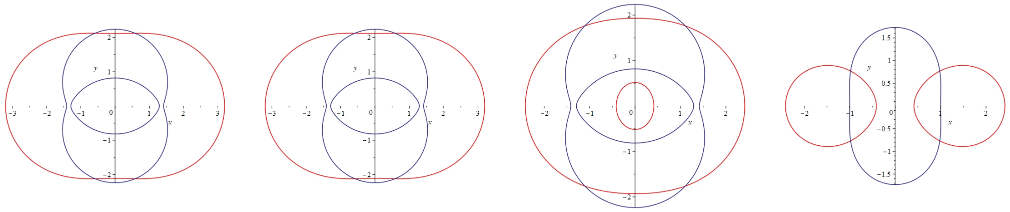
Using the command **Hessian** of Maple 2021, we show easily that the Hessian of a spiric curve is also a spiric curve. A couple of examples of the pair curve-Hessian is displayed in Figure 3, using the general equation

$$(x^2+y^2)^2 + ax^2 + by^2 + c = 0, \tag{2}$$

where $a,b,c \in \mathbb{R}$. The equation of the Hessian is then

$$(x^2+y^2)^2 + + \left(\frac{1}{6}a + \frac{1}{2}b\right)x^2 + \left(\frac{1}{6}b + \frac{1}{2}a\right)y^2 + \frac{1}{12}ab \tag{3}$$

Figure 3 show a few examples. Other configurations exist. In each case, the triple (a,b,c) is given; the original spiric is in red and its Hessian in blue.



(a) $(a,b,c) = (-8,-4,-2)$ (b) $(a,b,c) = (-10,-4,-2)$ (c) $(a,b,c) = (-6,-4,1)$ (d) $(a,b,c) = (-6,4,1)$

Figure 3: A spiric and its Hessian

Copying the data into a DGS[*] a hand-driven exploration is performed to check the points of inflexion, but a precise determination of these points requires the algebraic abilities of the CAS. A well-known theorem states that if $\mathcal{C}$ has points of inflexion, they are points of intersection of $\mathcal{C}$ with its Hessian; see [5,6]. According to the background of the students, various commands can be used, starting from **solve** to solve almost manually the system of equations (the output is often given using teh plac holder *RootOf* and the command **allvalues** has to be applied), and including **intersectcurves** (from the **algcurves** package). Checking whether the points of intersection which are determined are points of inflexion or not requires knowledge on curves given by an implicit equation which is not always taught. This work emphasizes once again the importance of the dialog between the educator and the technologies, and between the technologies, studied in [4].

We explore the relation between the shape of the original oval $\mathcal{C}$ and of its Hessian $\mathcal{H}$, also the relation between the two pairs of intersecting torus-plane,using the method of [1].

Keywords
Automated exploration, spiric curves, Cassini ovals, Hessian, inflexion points

References

[1] TH. DANA-PICARD. Technology as a bypass for a lack of theoretical knowledge, International Journal of Technology in Mathematics Education 11 (3), 101–109 (2005).
[2] TH. DANA-PICARD, G. MANN AND N. ZEHAVI. *From conic intersections to toric intersections: the case of the isoptic curves of an ellipse*, The Montana Mathematical Enthusiast 9 (1), 59–76 (2011).
[3] TH. DANA-PICARD, N. ZEHAVI AND G. MANN. *Bisoptic curves of hyperbolas*, International Journal of Mathematical Education in Science and Technology 45 (5), 762–781 (2014).
[4] TH. DANA-PICARD AND Z. KOVÁCS. *Offsets of Cassini ovals*, Preprint, 2021.
[5] J.J. CALLAHAN. *Advanced Calculus: A Geometric View*. Springer Science & Business Media, 2010.
[6]A.A. SWAMINATHAN. *Inflection Points in Families of Algebraic Curves*, Thesis, Harvard College, 2017. Downloadable: https://www.math.harvard.edu/media/swaminathan.pdf

[*] We used GeoGebra, freely downloadable from http:\geogebra.org

Applications of Computer Algebra – ACA 2021
Online | July 23-27, 2021
Session on *“Computer Algebra in Education”*

Automated exploration of envelopes and offsets with networking of technologies

Thierry Dana-Picard[1]***, Zoltán Kovács***[2] [ndp@jct.ac.il]

[1] Jerusalem College of Technology, Jerusalem, Israel
[2] The Private University College of Education of the Diocese of Linz, Linz, Austria

Envelopes of parameterized families of plane curves, of space curves, of surfaces, are an important topic both because of the mathematics involved and because of their applications (e.g. the determination of safety zones around sprinklers, robotic plants, Luna Park attractions, etc.). A drawback of this domain is the small number of its theorems, and the need to study numerous special cases [10]. Moreover, there exists 4 non-equivalent definitions of envelopes; see [3, 1].

The usage of technology makes the study of envelopes a live domain of study and may attract students to exploration and discovery (e.g., see [4, 5, 6]). A Dynamic Geometry System (DGS) provides an environment for automated exploration and discovery. In particular GeoGebra's companion package GeoGebra Discovery has a command for the determination of an envelope under certain conditions for the construction [7]. Nevertheless, the commands may not work in certain situations (such as non-polynomial data or higher degree polynomials). It may be then useful to transfer the data (the equations) to a Computer Algebra System, with which analytic solutions will be computed. The output may be afterwards transferred back to the DGS.

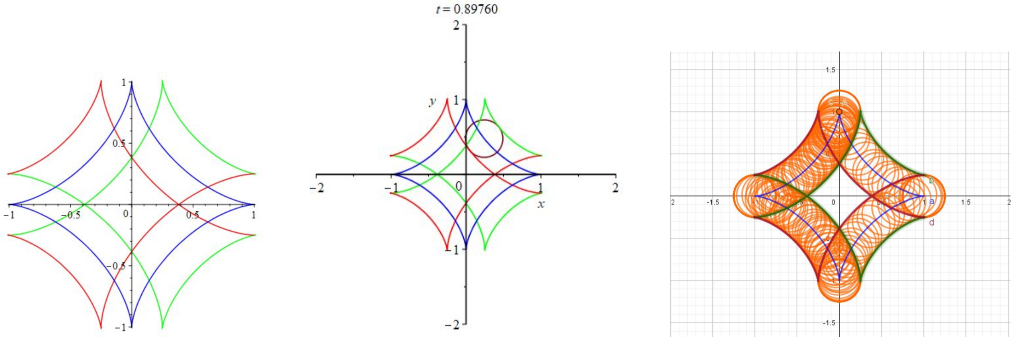
Let a parameterized family of plane curves $\mathcal{C}_t$ be given by the equation $F(x, y, t) = 0$. If an envelope exists, it is given by the solution of the system of equations

$$\begin{cases} F(x, y, t) = 0, \\ \frac{\partial F}{\partial t} F(x, y, t) = 0. \end{cases}$$

In a polynomial setting, the **solve** command of the CAS uses algorithms from the theory of Gröbner bases [8]. In various situations, it is possible to transform the given data into polynomial form. Then the CAS provides a parametric presentation of the envelope (which can be described as the disjoint union of several components). These equations are copied into the DGS for the final graphical presentation (e.g. using the **Curve** command of GeoGebra).

In this talk:

1. We show how this “networking” of technologies is used;
2. We analyze the differences between the animations provided by the CAS and the interactive exploration enabled by the DGS, and how to have profit of these differences.
3. We analyze the possible contradiction between the first intuition and the actual output, in particular with regards to the issue of safety zones evoked above. In Figure 1 we show a family of circles centred on an astroid. The envelope of the family is different from the hull enclosing all the circles in the family.



(a) (b) (c)

Figure 1: Envelope vs safety hull

Figure 1(a) shows the astroid and the envelope of a family of circles centred on it, with radius 1/4, after computations with Maple and implicit plot. Figure 1(b) is a snapshot of an animation obtained with Maple, Figure 1(c) shows the output of a mouse driven experimentation with GeoGebra, using in GeoGebra algebraic results from Maple, networking with the technologies. Figures 1(a)and 1(c) reveal different aspects: the last one has been obtained with an interactive exploration using the DGS. The algebraic description has been obtained as an offset of the astroid, namely the geometric locus of the points constructed as follows: for each point on the astroid, consider the normal at this point and the point at distance $\frac{1}{4}$ out of the astroid. The important difference between the 1^{st} and the last Figures is the arcs of circles appearing around the cusps the astroid. The analysis of these arcs requires strong zooming.

In [6], we studied offsets of a deltoid, here we perform similar work based on an astroid. Once again, new constructions of interesting plane curves appear.

The features and activities that we describe here show how to implement and develop the 4 C’s of Education in the 21st century [9]: Critical thinking, Creativity, Communication and Collaboration. If the first two C’s are human characteristics, the exploration that we propose requires the two last C’s both for humans and for machines and expands also the man-and-machine C’s. Strong zooming is a must in order to have an accurate conjecture of what happens, in particular regarding singular points.

Keywords
Automated exploration, Envelopes, Networking, 4 C’s of Education

References

[1] Botana, F. and Recio, T.: A propósito de la envolvente de una familia de elipses, Boletin de la sociedad Puig Adam 95 (2013), 15–30.

[2] F. Botana and T. Recio, Some issues on the automatic computation of plane envelopes in interactive environments. *Mathematics and Computers in Simulation* **125**, 115–125 (2016).

[3] J.W. Bruce and P.J. Giblin, Curves and Singularities, Cambridge University Press (1992). Online https://doi.org/10.1017/CBO9781139172615 (2012).

[4] Th. Dana-Picard and N. Zehavi, Revival of a classical topic in Differential Geometry: the exploration of envelopes in a computerized environment, *International Journal of Mathematical Education in Science and Technology* **47**(6), 938–959 (2016).

[5] Th. Dana-Picard and N. Zehavi, Automated Study of Envelopes of 1-parameter Families of Surfaces. In *Applications of Computer Algebra 2015: Kalamata, Greece, July 2015*, I.S. Kotsireas and E. Martínez-Moro (eds.), 29–44. Springer Proceedings in Mathematics & Statistics (PROMS Vol. 198), 2017.

[6] Th. Dana-Picard and Z. Kovács, Networking of technologies: a dialog between CAS and DGS, *The electronic Journal of Mathematics and Technology* (eJMT) 15 (1), 2021. Available: https://php.radford.edu/~ejmt/deliveryBoy.php?paper=eJMT_v15n1p3

[7] Kovács, Z., Achievements and Challenges in Automatic Locus and Envelope Animations in Dynamic Geometry, Mathematics in Computer Science **13**, 131–141 (2019).

[8] A. Montes, *The Gröbner Cover*. Algorithms and Computations in Mathematics **27**, Springer Nature 2018.

[9] S. Chiruguru, *The Essential Skills of* 21^{st} *Century Classroom (4Cs)*, 2021. Available: https://www.researchgate.net/publication/340066140_The_Essential_Skills_of_21st_Century_Classroom_4Cs, DOI:10.13140/RG.2.2.36190.59201.

[10] R. Thom, Sur la théorie des enveloppes. *Journal de Mathématiques Pures et Appliquéées* **XLI** (2),177–192 (1962).

Applications of Computer Algebra – ACA 2021
Online | July 23-27, 2021
Session on *“Computer Algebra in Education”*

Is computer algebra ready for conjecturing and proving geometric inequalities in the classroom?

Zoltán Kovács[1]***, Tomás Recio***[2]***, Róbert Vajda***[3]***, M. Pilar Vélez***[2] [zoltan@geogebra.org]

[1] The Private University College of Education of the Diocese of Linz, Linz, Austria
[2] University Antonio de Nebrija, Madrid, Spain
[3] Bolyai Institute, Szeged, Hungary

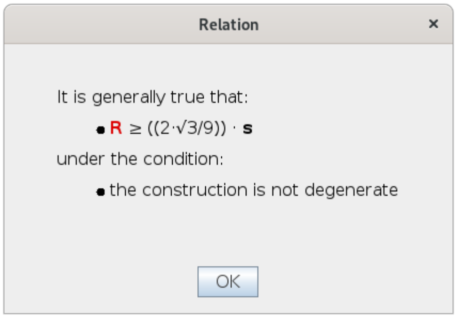
Supporting automated reasoning in the classroom has a long history in the era of computer algebra. Several systems have been developed and introduced as prototypes at various school levels during the last decades. A breakthrough in using computers to obtain automated proofs is still expected, even if some freely available systems offer easy access to such technical means.

In teaching geometry we refer to *GeoGebra* which became the de facto standard of a handy geometry toolset in many schools worldwide. It allows conjecturing and proving *equational* statements, including the geometric properties like parallelism, perpendicularity or equality of lengths of segments in a planar geometric figure [9, 13], and more recently, *inequational* theorems [16].

It is well-known that proving geometric inequalities is a more difficult scenario. Even if there were robust frameworks created in the last 30 years including *QEPCAD B* [6, 3], Reduce/*Redlog* [8], Maple/*RegularChains* [4], Maple/*SyNRAC* [10] or *Mathematica* [18], practical use of them was not yet in the focus of educational research. In our talk we introduce an extension of GeoGebra by adding a layer that is capable of using QEPCAD B (via the *Tarski* [17] system) to conjecture and prove, or directly prove some simple geometric inequalities.

In our extension we build on the classical way of translating the geometric setup into an algebraic system, based on the revolutionary work of Wu [19], Chou [5], and improved later by Recio and Vélez [14] with elimination theory. On the other hand, we partly use general purpose real quantifier elimination (RQE) methods to find the best possible geometric constants to conjecture and prove sharp inequalities between two expressions. Our implementation uses cylindrical algebraic decomposition (CAD) that promotes effective RQE. In fact, the translation of the geometric setup sometimes involves inequalities well, for example, when a point is put on a segment or inside a triangle, or angle bisectors are drawn.

Fig. 1 shows how the inequality $s \leq 3\sqrt{3}R$ (where s stands for the semiperimeter and R for the circumradius) can already be mechanically proven by our toolset in an intuitive way. The



It is generally true that:

- R ≥ ((2·√3/9)) · s

under the condition:

- the construction is not degenerate

Figure 1: A simple inequality that is automatically discovered and proven by GeoGebra Discovery

underlying semi-algebraic translation is shown if Fig. 2.

In our communication we do not go into the hidden technical difficulties, but refer to the paper [16] that focuses on the RQE related issues, and points to a large set of benchmarks based on our tool (including several examples from [1]). Instead, we focus on the practical use: how our work can be fruitful for the student and the teacher in a classroom.

Our experimental system is already capable of solving a large set of open questions in planar Euclidean geometry. But speed remains an important issue: we recall that solving a CAD problem has doubly exponential complexity in the number of variables (see [2, 7]).

GeoGebra Discovery is freely available at [11] for all three majors platforms (for Linux a 64 bit version and a Raspbian variant are published).

In our communication we will reflect on the potential impact of GeoGebra Discovery in the educational world. We will mention self-experimenting as well as student and teacher trainings to prepare for mathematics contests and exams. To illustrate our concept we will show some examples that are based on the books [1] and [15].

Keywords
Automated deduction in geometry, Inequalities, GeoGebra.

References

[1] O. Bottema, R. Djordjevic, R. Janic, D. Mitrinovic, and P. Vasic. *Geometric Inequalities*. Wolters-Noordhoff Publishing, Groningen, 1969.

[2] C. Brown and J. Davenport. The complexity of quantifier elimination and cylindrical algebraic decomposition. In *Proceedings of ISSAC '07*, pages 54–60. ACM, 2007.

[3] C. W. Brown. An overview of QEPCAD B: a tool for real quantifier elimination and formula simplification. *Journal of Japan Society for Symbolic and Algebraic Computation*, 10(1):13–22, 2003.

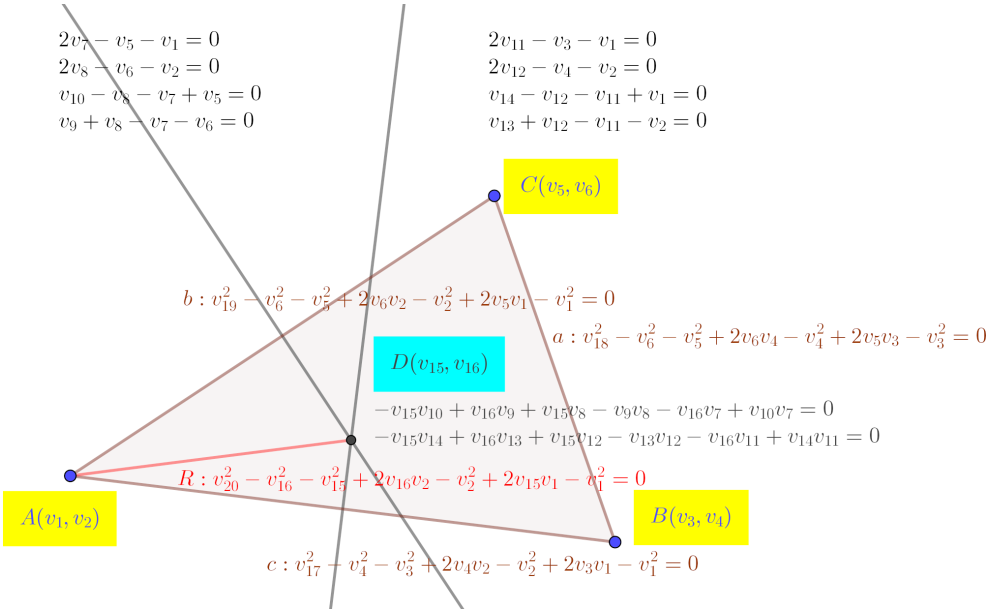

$2v_7 - v_5 - v_1 = 0$
$2v_8 - v_6 - v_2 = 0$
$v_{10} - v_8 - v_7 + v_5 = 0$
$v_9 + v_8 - v_7 - v_6 = 0$
$2v_{11} - v_3 - v_1 = 0$
$2v_{12} - v_4 - v_2 = 0$
$v_{14} - v_{12} - v_{11} + v_1 = 0$
$v_{13} + v_{12} - v_{11} - v_2 = 0$
$C(v_5, v_6)$
$b : v_{19}^2 - v_6^2 - v_5^2 + 2v_6v_2 - v_2^2 + 2v_5v_1 - v_1^2 = 0$
$a : v_{18}^2 - v_6^2 - v_5^2 + 2v_6v_4 - v_4^2 + 2v_5v_3 - v_3^2 = 0$
$D(v_{15}, v_{16})$
$-v_{15}v_{10} + v_{16}v_9 + v_{15}v_8 - v_9v_8 - v_{16}v_7 + v_{10}v_7 = 0$
$-v_{15}v_{14} + v_{16}v_{13} + v_{15}v_{12} - v_{13}v_{12} - v_{16}v_{11} + v_{14}v_{11} = 0$
$R : v_{20}^2 - v_{16}^2 - v_{15}^2 + 2v_{16}v_2 - v_2^2 + 2v_{15}v_1 - v_1^2 = 0$
$A(v_1, v_2)$
$B(v_3, v_4)$
$c : v_{17}^2 - v_4^2 - v_3^2 + 2v_4v_2 - v_2^2 + 2v_3v_1 - v_1^2 = 0$

Figure 2: Translation of the hypotheses of the geometric problem setting into an algebraic (or semi-algebraic) system

[4] C. Chen and M. M. Maza. Quantifier elimination by cylindrical algebraic decomposition based on regular chains. *Journal of Symbolic Computation*, 75:74–93, 2016.

[5] S. C. Chou. *Mechanical Geometry Theorem Proving*. D. Reidel Publishing Company, Dordrecht, Netherlands, 1988.

[6] G. E. Collins and H. Hong. Partial cylindrical algebraic decomposition for quantifier elimination. *Journal of Symbolic Computation*, 12:299–328, 1991.

[7] J. Davenport and J. Heintz. Real quantifier elimination is doubly exponential. *Journal of Symbolic Computation*, 5(1).

[8] A. Dolzmann and T. Sturm. Redlog: Computer algebra meets computer logic. *ACM SIGSAM Bulletin*, 31(2):2–9, 1997.

[9] M. Hohenwarter, Z. Kovács, and T. Recio. *Using Automated Reasoning Tools to Explore Geometric Statements and Conjectures*, pages 215–236. Springer International Publishing, Cham, 2019.

[10] H. Iwane, H. Yanami, and H. Anai. SyNRAC: a toolbox for solving real algebraic constraints. In *Proceedings of ICMS-2014. LNCS, vol. 8592*.

[11] Z. Kovács. GeoGebra Discovery. A GitHub project, 07 2020. https://github.com/kovzol/geogebra-discovery.

[12] Z. Kovács, T. Recio, P. R. Richard, S. V. Vaerenbergh, and M. P. Vélez. Towards an ecosystem for computer-supported geometric reasoning. *International Journal of Mathematical Education in Science and Technology*, 2020.

[13] Z. Kovács, T. Recio, and M. P. Vélez. Using automated reasoning tools in GeoGebra in the teaching and learning of proving in geometry. *International Journal of Technology in Mathematics Education*, 25(2):33–50, 2018.

[14] T. Recio and M. P. Vélez. Automatic discovery of theorems in elementary geometry. *Journal of Automated Reasoning*, 23:63–82, 1999.

[15] I. Reiman. *Fejezetek az elemi geometriából*. Typotex, Budapest, 2002.

[16] R. Vajda and Z. Kovács. GeoGebra and the *realgeom* reasoning tool. *CEUR Workshop Proceedings*, pages 204–219, 6 2020.

[17] F. Vale-Enriquez and C. Brown. Polynomial constraints and unsat cores in TARSKI. In *Mathematical Software – ICMS 2018. LNCS, vol. 10931*, pages 466–474. Springer, Cham, 2018.

[18] Wolfram Research, Inc. Mathematica, version 12.1, 2020. Champaign, IL.

[19] W. T. Wu. On the decision problem and the mechanization of theorem proving in elementary geometry. *Scientia Sinica*, 21:157–179, 1978.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Computer Algebra in Education"*

Can I bring my calculator to the exam? Some reflections on the abstraction level of CAS

Eugenio Roanes-Lozano[1,2] [eroanes@ucm.es]

[1] Instituto de Matemática Interdisciplinar (IMI), Universidad Complutense de Madrid, Spain
[2] Departamento de Didáctica de las Ciencias Experimentales, Sociales y Matemáticas, Facultad de Educación, Universidad Complutense de Madrid, Spain

For many years, the standard answer to the question "Can I bring my calculator to the exam?" (regarding the college entrance exams in Spain –denoted EvAU [1]) was: "Yes. But it will be useless".

From the maths teachers' point of view, we could classify the questions of maths exams in four classes:

- **Numerical computations and substitutions in formulae:**
  They arise in all fields of maths (algebra, geometry, analysis, astronomy,...). They were solved in the past with pen and pencil and sometimes using logarithm tables, slide rules, etc. They can be solved with a (classic) calculator.
  Example 1: Calculate the final price of a skirt tagged a price of 23.5 Euros (VAT excluded) if the VAT is 21% and it has a 10% discount.

- **Symbolic computations (simplifications, expansions, concatenation of algebraic calculations, etc.):**
  Example 2: Simplify $(x+y)^2-(x-y)^2$.
  Example 3: Analyse when a certain parameter-depending linear system has solutions and find them in such case.
  Example 4: Draw a function by computing its zeroes, maxima and minima, asymptotes, inflection points, etc. In the EvAU these functions are normally trickily chosen so that they have, for instance, two very close zeroes [2] (in order a graphic calculator to be useless).
  Example 5: Find the integral $\int x \cdot log(x)\ dx$ (it is straightforward using the integration by parts method).
  In the past they could only be solved by hand. Now these tasks can be completed by computer algebra systems (CAS), that are available for computers, tablets and smartphones.

- **Theoretical questions regarding mathematical formulae:**
  Example 6: What is the cube of a binomial.
  Example 7: What is $sin(2x)$ equal to?
  Example 8: What is the determinant of a 3×3 matrix (Sarrus rule)?
  Example 9: What is the derivative of the product of two functions?
  All the mentioned tasks can also be completed by a CAS.

- **Theorem proving:**
  There are two main lines regarding research in theorem proving: logic deduction from the axioms (using deduction rules), applicable to all fields of mathematics, and automatic theorem proving in geometry [3] (using algebraic methods) [4–6]. CAS are the key tool for the latter line of research. The main problem is the readability of the proofs produced by the two lines of research aforementioned and their lack of elegance (synthetic proofs and proofs based on brilliant ideas can't be developed these ways). But this is not the topic of this talk.

From the CAS point of view (unlike what happens from the teacher's point of view) there is no difference between the questions in the second and third classes: they can be completed by the CAS just performing symbolic computations. They are of an abstraction level [7] higher than those of the first class (as they deal with non-assigned variables –variables in the mathematical sense, not in the computational sense).

The case of Example 9 is specially interesting, as it reaches an even higher abstraction level: the CAS deals in this case with general functions, not only with already declared functions, themselves depending on non-assigned variables. Many maths teachers and CAS users are unaware of such possibility of CAS. It can be easily introduced to, for instance, *Maple*[*] [8–12] and computed by this CAS:

```
> diff(f(x)*g(x),x);
```

$$\left(\frac{d}{dx}\, f(x)\right) g(x) + f(x) \left(\frac{d}{dx}\, g(x)\right)$$

Summarising, CAS have reached an unprecedented abstraction level with many possibilities in different fields. As a consequence, assessment in maths education depends on the availability of technological tools: a CAS can be used to solve symbolic problems and also as a technological live cheat sheet (in theoretical questions).

Keywords
Computer algebra, Abstraction level, Assessment.

References

[1] I. Munat Hervás, *Problemas de Selectivdad de Matemáticas II. Comunidad de Madrid. Por examen y resueltos (2000-2021)*. –, Madrid, 2021.
[2] W. Koepf, Numeric versus symbolic computation. In *Recent developments in complex analysis and computer algebra*, R. P. Gilbert, J. Kajiwara, Y. S. Xu (eds.), pp. 179-203. Kluwer, London–Dordrecht–Boston, 1999.

[*] *Maple* is a trademark of Waterloo Maple Inc.

[3] F. BOTANA; M. HOHENWARTER; P. JANIČIĆ; Z. KOVÁCS; I. PETROVIĆ; T. RECIO; S. WEITZHOFER, Automated Theorem Proving in GeoGebra: Current Achievements. *Journal of Automated Reasoning* **55**, 39–59 (2015).

[4] B. BUCHBERGER, Applications of Gröbner Bases in Non-Linear Computational Geometry. In *Mathematical Aspects of Scientific Software*, J. R. Rice (ed.), pp. 59–87. Springer, New York, 1987.

[5] W. WEN-TSÜN, On the Decision Problem and the Mechanization of Theorem Proving in Elementary Geometry. *Scientia Sinica* **21**, 157–179 (1978).

[6] S. C. CHOU, *Mechanical Geometry Theorem Proving*. D. Reidel Publishing Company, Dordrecht, 1988.

[7] S. M. WATT, On the Future of Computer Algebra Systems at the Threshold of 2010. In *Proc. Joint Conference of ASCM 2009 and MACIS 2009: Asian Symposium of Computer Mathematics and Mathematical Aspects of Computer and Information Sciences, (MACIS 2009), December 14-17 2009, Fukuoka, Japan*, pp. 422-430, COE Lecture Note Vol. 22, Kyushu University, Fukuoka, Japan, 2009.

[8] L. BERNARDIN; P. CHIN; P. DEMARCO; K. O. GEDDES; D. E. G. HARE; K. M. HEAL; G. LABAHN; J. P. MAY; J. MCCARRON; M. B. MONAGAN; D. OHASHI; S. M. VORKOETTER, *Maple Programming Guide*. Maplesoft, Waterloo Maple Inc., Waterloo, Canada, 2020.

[9] R. CORLESS, *Essential Maple. An Introduction for Scientific Programmers*. Springer, New York, 1995.

[10] A. HECK, *Introduction to Maple*. Springer, New York, 2003.

[11] MAPLESOFT, *Maple User Manual*. Maplesoft, Waterloo Maple Inc., Waterloo, Canada, 2021.

[12] E. ROANES-MACÍAS; E., ROANES-LOZANO, *Cálculos Matemáticos por Ordenador con Maple V.5*. Editorial Rubiños-1890, Madrid, 1999.

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

From hidden invariants to multiple solutions using computer algebra tools: two activities for pre-service teachers

I. Sinitsky[1]**, *M. Sinitsky***[1] [sinitzsk@gordon.ac.il]

[1] Gordon Academic College of Education, Haifa, Israel

It is well known that the study of geometry involves a number of difficulties, one of which is the sharp switch from the intuitive exploration of the properties of geometrical objects to the necessity of rigorous proofs in the more advanced stages of learning geometry. To smooth this transition, modern curricula suggest involving learners in open-type activities through which they can explore various geometrical objects and the properties that arise in series of different geometrical situations.

Pre-service teachers do understand, at least in theory, the importance of both open-type and computer-assisted learning; a good portion of them are enthusiastic to take part in such a process. However, their initial trials often lead to early frustration as already during the initial steps of their inquiry search for the solution they encounter difficulty ("I have no idea how to get started!").

To overcome this difficulty, we have designed a set of open-ended activities, each of which begins with a very simple situation and then develops further to explore some profound - and often surprising - invariant properties. Here, we present two examples of such activities - portioning polygons and constructing Diophantine-type polygons - with a focus on how using computer algebra tools (GeoGebra in our trial) influences both students' reasoning and the results they achieve. The first activity, “From two to n, from one to infinity,” deals with dividing a regular n-gon into k congruent pieces (or at least into k pieces with the same area). The origin/starting point is the partition of a regular n-sided polygon into n equal triangular pieces. Further exploration will lead to numerous additional solutions, depending on the value of k for the given regular polygon, and may even lead to a procedure for how to divide any arbitrary combination of n and k [1]. In any case, the discovery of area invariance through the use of GeoGebra provides the students breakthrough understanding of the infinite ways of division for every value of k.

The second activity described, “From nine to one, from one to infinity,” is a three-step puzzle. The first step asks for the construction of polygons with an integer area from 12 whole toothpicks [2]. The immediately obvious area of 9 units (the square) can be easily decreased to 5 units even in the set of rectilinear polygons [3], and some students are able to discover some polygons with even less area by using "manual" manipulations. However, to arrive at a large number of novel solutions, they typically need to explore perimeter invariance for the constructions in a dynamic environment, whereby they discover that the number of possible solutions is surprisingly huge - although finite. In the third part, the combination of two invariants pave the way to construct an infinite set of Diophantine - and even equilateral (!) - polygonal solutions.

Keywords
polygon divisions, Diophantine polygon construction, invariants, student reasoning

References

[1] I. SINITSKY; M. STUPEL; M. SINITSKY, Pizza again? On the division of polygons into sections with a common origin. *International Journal of Mathematical Education in Science and Technology* **49**(2), 281–293 (2017).
[2] N. YOSHIGAHARA, *Puzzles 101.* A K Peters, 2004.
[3] MATCHSTICK PUZZLES, A collection. Extreme # 121(2019). `http://matchstickpuzzles.blogspot.com/2013/12/121-create-smallest-area-with-12-sticks.html`

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Computer Algebra in Education*

Undergraduate Mathematics: a journey from a face-to-face to a remote teaching, learning and assessment

Discussion

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

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

The goal of this discussion is to bring together ideas for enhancing remote teaching, learning and assessment (TLA) of undergraduate mathematics. There exist

- widely spread/applied methodological principles and approaches in face-to-face mathematics education at colleges and universities;

- a great diversity of good practices in face-to-face mathematics education with and without application of Computer Algebra Systems (CAS);

- 3-semester experience in the TLA of undergraduate mathematics in remote learning environment.

We live in uncertain times. It is important to stay informed on the pressing issues in higher education. What kind of issues appeared and need to be discussed and experience to be exchanged:

- difficulties met by teachers and learners;

- lack of relevant tools and platforms;

- methodological issues: relevant teaching methods, learning strategies and assessment criteria;

- necessity for re-design of learning resources: innovative learning resources and relevant exam questions;

- the increasing role of CAS;

- ...

During the discussion around remote educational process participants could express their opinion about the "lessons learned from the pandemic about effective teaching" formulated by Steven Mintz ([1]) and add their own lessons:

- Teaching online is tough work.
- It's easy for online students to disengage, self-isolate and fall off track.
- Social and emotional issues are as important as course content.
- Coverage and pacing pose a big challenge.

It is expected that remote education will persist after the pandemic. Steven Mintz ([1]) and Janice Florent ([2]) listed the following eight ethical issues:

1. **Equity**: How to ensure that every student has an equal opportunity to learn and to fully participate in our online courses.
2. **Learner diversity**:How to address the special challenges that e-learning poses.
3. **Support**:How to ensure that students have the ready access to the academic, technological, mental health and other supports that they need to succeed.
4. **Feedback and responsiveness**:Making sure that students receive the guidance and feedback they need to succeed academically.
5. **Privacy**:How to ensure that students' right to privacy is protected.
6. **Netiquette**:How to ensure that all participants in the class behave in a civil, respectful manner.
7. **Assessment**:How to maintain academic integrity in an online environment.
8. **Intellectual property**:What rules should govern respect for copyright in online classes.

In the 2030 Digital Compass ([3]) it is underlined that education is being engulfed to the center of the digital vortex. It stays there: "Those who saw digital technologies as tools to enable traditional teaching and learning processes will begin to realize how much more potential they have. The context allows a better understanding of McLuhan, who in the last century warned that "the medium is the message." Educational changes, infused with digital technologies, are radical, rapid and profound. Last century, education aimed to provide mastery of one set of techniques and skills. In this century, although such training remains necessary, it is insufficient. We are moving toward a new aim: the ability to learn continuously, with awareness about how we learn. . . . "

Keywords
Undergraduate mathematics, Remote teaching-learning-assessing, CAS, Bloom's taxonomy.

References

[1] Steven M. 2021, What the Pandemic Should Have Taught Us About Effective Teaching. The lessons that ought to shape post-pandemic pedagogy. https://www.insidehighered.com/blogs/higher-ed-gamma/what-pandemic-should-have-taught-us-about-effective-teaching

[2] Janice Florent, June 2021. https://cat.xula.edu/food/what-the-pandemic-should-have-taught-us-about-effective-teaching/

[3] 2030 Digital Compass: the European way for the Digital Decade Communication, March 2021. https://eufordigital.eu/library/2030-digital-compass-the-european-way-for-the-digital-decade/

.

Challenges and opportunities in remote teaching, learning and assessment of undergraduate mathematics

Elena Varbanova[1]**,*Magdalina Uzunova***[2] [elvar@tu-sofia.com]

[1] 1Faculty of Applied Mathematics and Informatics, Technical University of Sofia, Bulgaria
[2] Faculty of Transport Engineering, University of Architecture, Civil Engineering and Geodesy, Bulgaria

Almost all teachers spent 3 semesters teaching remotely. The triad teaching-learning-assessing (TLA) has been provoked. Pedagogical challenges have been inevitable: innovative learning resources containing different ways and prototypes - to help students grasp the material acquiring essential knowledge and skills, had to be delivered. Visualization and step by step technique proved to be helpful for effective teaching and learning. Interactivity and non-assessed assignments appeared to be necessary to track students' learning trajectory. The assessment challenge has been of equal importance. Innovative assignments/questions that require students to apply knowledge, thinking skills and critical thinking have been developed. As some students need more time to master essential skills and knowledge it was necessary to design classes to allow for more personalization of pace. As a whole, learning outcomes and educational goals has to be re-considered and clearly described for the purpose of higher order learning in case of remote TLA process. Computer Algebra Systems proved to be a basic instrument for implementation of new methodological approaches in a remote TLA process. The latter is an iterative process: changes in one of the components of TLA require adequate changes in the other two. Such effects will be illustrated. Concerning opportunities: they can be seen in the innovative learning resources and assignments we have created; it has to be mentioned that the learners are co-creators of the innovations.

Keywords
Undergraduate mathematics, remote teaching, pedagogical and assessment challenges, CAS

References

[1] Steven M. 2021, What the Pandemic Should Have Taught Us About Effective Teaching. The lessons that ought to shape post-pandemic pedagogy.

https://www.insidehighered.com/blogs/higher-ed-gamma/what-pandemic-should-have-taught-us-about-effective-teaching

[2] 2030 Digital Compass: the European way for the Digital Decade Communication, March 2021.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Computer Algebra in Education*

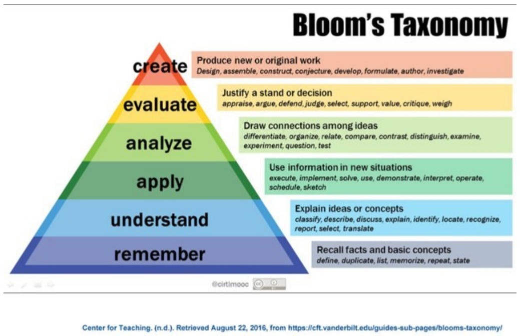
An Automated Symbolic Package to Enhance Higher Order Thinking Skills (HOTS): Critical Thinking

Yuzita Yaacob[1], ***Khairina Atika Mohd. Zawawi*** [1] [yuzita.yaacob@gmail.com]

[1]Faculty of Technology and Information Science, Universiti Kebangsaan Malaysia

The aim of this Computer Algebra System-Critical Thinking (CAS-CT) project is to enhance Higher Order Thinking Skills (HOTS) (critical thinking) by applying Problem Based Learning Method (PBLM) [1] using a symbolic package (named as i-phys 2.0). The focus area of i-phys 2.0 is physics (force and motion) for high school students in Malaysia. The technical design of the development of i-phys 2.0 is based on the CAS pedagogy characteristics concept (i.e., interactivity, visualization, experimentation, step by step technique, multiple representations and white box/black box principle) [2]. The learning model to develop i-phys 2.0 is based on Bloom's Taxonomy [3] (see Figure 1) . i-phys 2.0 is also design for web based users wherein teaching and learning can be done online. PBLM is applied using i-phys 2.0 through teamwork to sharpen the student's ability to criticize opinion, express thoughtful ideas and give relevant proposals to solving problems. This is important as the market demand nowadays not only require workers that possess academic excellence but also generic skills (i.e., critical thinking, teamwork, positive thinking and leadership traits) [4]. The mastery of scientific numeracy and literacy via the application of i-phys 2.0 provide solid foundation to develop diversity skills to seize job opportunities particularly in the field related to STEM (Science, Technology, Engineering and Mathematics). i-phys 2.0 is also intended to nurture self confidence, fun in learning and strong desire to continuously acquiring knowledge especially in the work life. Usability testing of i-phys 2.0 is based on attributes: effectiveness, learnability and satisfaction. Each attribute contains usability criteria that is CAS pedagogy characteristics concept and tested using Pre Experimental One-Shot Case Study. After treatment using i-phys 2.0, post testing is conducted to determine the assessment level of achievement score in critical thinking. I-phys 2.0 is a continuation and enhancement of i-phys developed by Hazlina [5].

Keywords
Symbolic package, Critical thinking, Bloom's taxonomy, Problem Based Learning Method (PBLM).



Bloom's Taxonomy

create — Produce new or original work
Design, assemble, construct, conjecture, develop, formulate, author, investigate

evaluate — Justify a stand or decision
appraise, argue, defend, judge, select, support, value, critique, weigh

analyze — Draw connections among ideas
differentiate, organize, relate, compare, contrast, distinguish, examine, experiment, question, test

apply — Use information in new situations
execute, implement, solve, use, demonstrate, interpret, operate, schedule, sketch

understand — Explain ideas or concepts
classify, describe, discuss, explain, identify, locate, recognize, report, select, translate

remember — Recall facts and basic concepts
define, duplicate, list, memorize, repeat, state

@cirtlmooc

Center for Teaching. (n.d.). Retrieved August 22, 2016, from https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/

Figure 1: Bloom's taxonomy

References

[1] Newby T. J.; Stepich D. A.;Lethman J. D.;Russell J. D.; Leftwich A. O. 2011. *Educational Technology for Teaching and Learning. Fourth Edition.*. Pearson Education Inc.

[2] Yuzita Yaacob;Wester, M.;Steinberg, S. 2010. *Towards the Development of an Automated Learning Assistant for Vector Calculus: Integration over Planar Regions*. International Journal for Technology in Mathematics Education 17(2):81-86.

[3] Benjamin Bloom. 2001., *A Taxonomy for Learning, Teaching and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives.*.

[4] Seminar Refleksi Latihan Mengajar (KPR 3012). 2016. , *Pelaksanaan Kemahiran Berfikir Secara Kritis dan Kreatif. Cikgupija92.blogspot.com.*.

[5] Hazlina Awang Lah. 2014., *Pakej Simbolik Pendidikan Fizik (i-phys) Berasaskan Sistem Algebra Komputer. Tesis Doktor Falsafah. Universiti Kebangsaan Malaysia.*.

.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Computer Algebra in Education"*

CAS Tools for teaching function discontinuities

David G. Zeitoun[1]*,* ed.technologfie@gmail.com]

[1] Department of Mathematics, Orot College of Education, Elkana, D.N. Hare Efraim 44148, Israel

Proving that a function is continuous at a given point using the epsilon-delta definition is a difficult task for the student. Proving that the function is not continuous at a given point using the negation of the delta –epsilon definition is even more difficult.

In this work, we present new tools and applets from a computer algebra system (CAS) to enhance understanding of function discontinuities. The CAS assists the teacher at three levels (See [1];[2]):

- enouncing the basic definition of continuity/discontinuity;
- proving properties;
- helping to solve exercises.

We analyse the usage of the CAS (Geogebra) for the understanding of the definitions of discontinuity and various properties and present new CAS tools, commands and templates, such as a *control rectangle* for the visualisation of the definition of the continuity and discontinuity ([3]). The animations based on the control rectangle help to understand the delta-epsilon definition. We recall that Heine's theorem states that given any sequences (x_n) converging to a given point x_0, if the sequence $f(x_n)$ converges to $f(x_0)$ then f is continuous at x_0 .

Heine's theorem is hard to use in a proof of limit continuity at a point because we need to check the limit for any sequence. However, this definition of the limit permits to check if the function f(x) is not continuous at $x = x_0$. If two convergent sequences x_n and y_n both convergent to $x = x_0$, then if $lim(f(x_n)$ is different from $lim(y_n)$ $f(x)$ is not continuous at $x = x_0$. The Heine theorem allows to prove easily that a function is discontinuous at a point.

We address the following issues:

1. The δ ϵ - definition is difficult to understand intuitively and it is far from the intuitive understanding of the continuity and the discontinuity.

2. Moreover the δ ϵ definition involves inequalities and requires algebraic knowledge in order to solve exercises. Therefore, the proofs of limit, continuity at a point is difficult for the student.

3. The definition of discontinuity may be taken from the δ ϵ - definition. It require to find a value of ϵ such that for any value of δ ,$|x - x_0| < \delta$ and $|f(x) - f(x_0)| > \epsilon$. This definition is the negation of the δ ϵ - definition of the continuity. So, the first difficulty for the student of this definition is to formulation the negation sentence of the continuity definition.

Keywords
Function discontinuity, CAS tools

References

[1] GIRALDO, V. AND CARVALHO, L.M. , *Local Straightness and Theoretical-Computational Conflicts: Computational Tools on the Development of the Concept Image of Derivative and Limit*, Proceedings of CERME 3, available: http://www.dm.unipi.it/~didattica/CERME3/proceedings/Groups/TG9/TG9_Giraldo_cerme3.pdf

[2] DUVAL, R., *The cognitive analysis of problems of comprehension in the learning of mathematics*, Educational studies in mathematics 61, 103-131. https://doi.org/10.1007/s10649-006-0400-zl

[3] ZEITOUN D.G,, DANA-PICARD, TH., In *Accurate visualization of graphs of functions of two real variables, International Journal of Computational and Mathematical Sciences 4(1), 1–11* . .

S12. Algebraic and Algorithmic Aspects of Differential and Integral Operators Session (AADIOS)

Organized by

Moulay Barkatou, Thomas Cluzeau, Clemens Raab and Georg Regensburger

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)”*

The global and weak global dimensions of algebras of integro-differential operators

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

We talk about recent results on computation of the global and weak global dimensions of the algebras of polynomial integro-differential operators $\mathbb{I}_n$, the Jacobian algebras $\mathbb{A}_n$ and their factor algebras. [1].

Keywords
the global dimension, the weak global dimension, the algebra of integro-differential oprators

References

[1] V. V. Bavula, The global dimension of the algebras of polynomial integro-differential operators $\mathbb{I}_n$ and the Jacobian algebras $\mathbb{A}_n$. *J. Algebra Appl.* **19**(2), 2050030, 28pp. (2020).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

The Kernel-Method and Automated Positive Part Extraction

Manfred Buchacher[1], ***Manuel Kauers***[1] [manfred.buchacher@jku.at]

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

Keywords
Lattice Walks, Generating Functions, Functional Equations, Kernel-Method, D-Finiteness

A lattice walk is a sequence $P_0, P_1, \ldots, P_n$ of points in $\mathbb{N}^d$. The points P_0 and P_n are its starting and end point, respectively, n is its length, and the consecutive differences $P_{i+1} - P_i$ are its steps. Fixing a starting point P and a set S of admissible steps combinatorialists ask for the number $f(Q, n)$ of walks in $\mathbb{N}^d$ that start at P, consist of n steps, all taken from S, and end at Q: Are there nice formulas for these numbers? What is their asymptotics as n goes to infinity? In answering these questions it is helpful to study the associated generating function

$$F(x,t) = \sum_{n\geq 0} \left(\sum_{P\in\mathbb{N}^d} f(P,t)x^P \right) t^n \in \mathbb{Q}[x][[t]]$$

and the functional equation it satisfies and to decide whether it satisfies a linear differential equation with polynomial coefficients or not. Mishna [1], [2] and Bousquet-Mélou [2] initiated a systematic study of this problem for walks restricted to $\mathbb{N}^2$ whose steps are taken from a subset S of $\{-1,0,1\}^2$ and introduced a method involving elementary power series algebra for proving D-finiteness of the generating functions of some instances of this problem. Bousquet-Mélou et al. [3] generalized it to walks with steps not necessarily restricted to $\{-1,0,1\}^2$. We show how this method can be extended and automatized using Gröbner bases and a generalized Newton-Puiseux algorithm.

References

[1] MARNI MISHNA, *Classifying Lattice Walks Restricted to the Quarter Plane.* Journal of Combinatorial Theory, Series A Vol 116(2): 460–477, 2009.
[2] MARNI MISHNA, MIREILLE BOUSQUET-MÉLOU. *Walks with Small Steps in the Quarter Plane.* Algorithmic Probability and Combinatorics, Special Volume of the Contemporary Mathematics Series of the AMS 520, 1–40, 2010.
[3] ALIN BOSTAN, MIREILLE BOUSQUET-MÉLOU, STEVEN MELCZER, *Counting Walks with Large Steps in an Orthant.* Journal of the European Mathematical Society, to appear.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

Holonomic Polynomial Sequences I: Degree Growth

***Jason P. Bell*[1]*, Shaoshi Chen*[2]*, Daqing Wan*[3]*, Rong-Hua Wang*[4] *and Hang Yin*[5] [schen@amss.ac.cn]

[1] Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada
[2] KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, 100190, China
[3] Department of Mathematics, University of California, Irvine, CA 92697, USA
[4] School of Mathematical Sciences, Tiangong University, Tianjin, 300387, China
[5] Institute of Mathematics, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, 100190, China

A sequence $P_n(x)$ of polynomials in x is holonomic (P-recursive) if it satisfies a linear recurrence with polynomial coefficients in x and n. Many polynomial sequences from combinatorics, representation theory and number theory are shown to be holonomic. It is natural and fundamental to study the degree pattern of holonomic polynomial sequences. We will present a classification of the degree growth of such sequences and explain two applications related to combinatorial identities and exponential sums over finite fields respectively.

Keywords
Holonomic sequences, Degree structure, Vanishing sums, Exponential sums

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

Strategies for linear rewriting systems: link with parallel rewriting and involutive divisions

Cyrille Chenavier[1] [cyrille.chenavier@unilim.fr]

[1] XLIM, Université de Limoges, Limoges, France

In this talk, I will present a joint work with Maxime Lucas [1]. It concerns rewriting systems whose underlying set of terms is equipped with vector space operations. In [1], we introduce parallel rewriting relations, which are rewriting relations compatible with the vector space operations, as well as rewriting strategies, which consist in choosing one rewriting step for each reducible basis element of the space. I will illustrate this framework with rewriting systems over rational Weyl algebras. In particular, I will relate involutive divisions to rewriting strategies over rational Weyl algebras, and explain how involutive sets induce confluent rewriting systems over rational Weyl algebras using strategies.

Keywords
Confluence, parallel rewriting, rewriting strategies, involutive divisions.

References

[1] C. CHENAVIER, M. LUCAS, *Strategies for linear rewriting systems: link with parallel rewriting and involutive divisions*. arXiv:2005.05764.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)”*

Symbolic integration on planar differential foliation

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

Université de Bourgogne, Dijon, France

We consider the problem of symbolic integration of $\int G(x, y(x))dx$ where G is rational and $y(x)$ is a non algebraic solution of a differential equation $y'(x) = F(x, y(x))$ with F rational. As y is transcendental, the Galois action allows to introduce a parameter $I(x, h) = \int G(x, y(x, h))dx$. We will prove that the function I is either differentially transcendental in h or satisfies a linear differential equation in h whose homogeneous part has constant coefficients. We will present an algorithm to compute such equation given a priori bound on their order and coefficient degree.

Keywords
Symbolic integration, creative telescoping, differential equations

References

[1] T. COMBOT; G.CHÈZE, Symbolic Computations of First Integrals for Polynomial Vector Fields. *Foundations of Computational Mathematics* **20**(4), 681–752 (2020).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)”*

Differential algebraic generating series of walks in the quarter plane

Thomas Dreyfus [dreyfus@math.unistra.fr]

[1] CNRS, Université de Strasbourg, France

To a walk confined in the quarter plane we may attach a generating series. The series depends upon three variables and a classical problem is to determine whether this series is solution of algebraic and/or differential equations. In this talk we will explain a very surprising result: the generating series is solution of an algebraic differential equation in one of its variable, if and only if it is solutions of an algebraic differential equation in each of its variable.

Keywords
Elliptic functions, Walks in the quarter plane

References

[1] T. DREYFUS, *Differential algebraic generating series of weighted walks in the quarter plane*.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

Two Complete Reduction Systems for Integration

Hao Du[1,2]***, Clemens G. Raab***[1] [duhao@amss.ac.cn]

[1] Institute for Algebra, Johannes Kepler University (JKU), Altenberger Straße 69, 4040 Linz, Austria
[2] School of Sciences, Beijing University of Posts and Telecommunications (BUPT), Beijing 100876, China

We apply Norman's completion process [1] to the Risch-Norman integration method [2] instead of using heuristic degree bounds to find antiderivatives in the differential polynomial ring generated by the given special functions. However, the behaviour of the completion process depends not only on the ring, but also on the ordering selected for terms. It may happen that the completion process does not terminate and yields an infinite number of reductions rules, which makes it hard to determine a complete reduction system. In such a case, one has to find finitely many formulae to denote the infinite number of reduction rules. By fixing adapted orderings, we present complete reduction systems for two families of functions satisfying second-order differential equations. In addition, they allow us to find rigorous weighted degree bounds for the antiderivatives.

Keywords
Completion process, Risch-Norman algorithm, Symbolic integration.

References

[1] ARTHUR C. NORMAN, A Critical-Pair/Completion based Integration Algorithm. *Proc. ISSAC' 90*, pp. 201–205, 1990.
[2] ARTHUR C. NORMAN; P. M. A. MOORE, Implementing the New Risch Algorithm. *Proc. 4th International Colloquium on Advanced Computing Methods in Theoretical Physics*, pp. 99–110, 1977.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)”*

Rota’s Program on Algebraic Operators

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

[1]School of Mathematics and Statistics, Lanzhou University, Lanzhou, Gansu 730000, P. R. China
[2]Department of Mathematics and Computer Science, Rutgers University, Newark, NJ 07102, United States

Linear operators satisfying various algebraic operator identities have appeared in mathematical research, including endomorphisms, derivations and Rota-Baxter operators. Many years ago, G.-C. Rota proposed a program to determine all such linear operators [1]. After an extended period of dormant, progress on this program picked up speed in recent years, thanks to perspectives from operated algebras, rewriting systems and Gröbner-Shirshov bases. These advances were achieved in a series of papers from special cases to more general situations [2,3,4]. These perspectives also indicate that Rota’s insight can be manifested very broadly, for other algebraic structures such as Lie algebras, and further in the context of operads. This talk presents motivation, early developments and recent advances on Rota’s program for linear operators on associative algebras and Lie algebras [5].

Keywords
Operator identity, Rewriting system, Gröbner-Shirshov basis

References

[1] G.-C. ROTA, Baxter operators, an introduction, In *Gian-Carlo Rota on Combinatorics, Introductory papers and commentaries*, J. Kung (eds.), 504-512, Birkhäuser, Boston, 1995.
[2] L. GUO, W. SIT AND R. ZHANG, Differential type operators and Gröbner-Shirshov bases, *J. Symbolic Comput.* **52**, 97–123 (2013).
[3] X. GAO, L. GUO, W. SIT AND S. ZHENG, Rota-Baxter type operators, rewriting systems and Gröbner-Shirshov bases, *J. Symbolic Comput.*, accepted.
[4] X. GAO AND L. GUO, Rota’s Classification Problem, rewriting systems and Gröbner-Shirshov bases, *J. Algebra* **470**, 219-253 (2017).
[5] X. GAO, L. GUO AND H. ZHANG, On Rota’s classification problem for Lie algebras, in preparation.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)”*

Linear PDE with constant coefficients

Marc Härkönen[1]***, Rida Ait El Manssour***[2]***, Bernd Sturmfels***[2,3] [harkonen@gatech.edu]

[1] School of Mathematics, Georgia Institute of Technology, Atlanta, USA
[2] Max Planck Institute for Mathematics in the Sciences, Leipzig, Germany
[3] Department of Mathematics, University of California at Berkeley, Berkeley, USA

In an undergraduate differential equations course we learn to solve a homogeneous linear ordinary differential equation with constant coefficients by finding roots of its characteristic polynomial. Thus the problem of solving an ODE is reduced to factoring a univariate polynomial. This simple idea was generalized in the 1960s for systems of linear PDE. The celebrated Fundamental Theorem by Ehrenpreis and Palamodov asserts that all solutions to a system of PDE can be represented by a finite sum of integrals over certain algebraic variety. This representation is strongly connected to the geometry of schemes or coherent sheafs corresponding to polynomial ideals or modules. In this talk I will review some of the main historical results, along with some recent advances in symbolic and numerical algorithms.

Keywords
Partial Differential Equations, Algebraic Geometry, Numerical Algebraic Geometry

References

[1] R. Ait El Manssour; M. Härkönen; B. Sturmfels, *Linear PDE with constant coefficients*, **arXiv:2104.10146** (2021).
[2] Y. Cid-Ruiz; J. Chen, *Primary decomposition of modules: a computational differential approach*, **arXiv:2104.03385** (2021).
[3] J. Chen; M. Härkönen; R. Krone; A. Leykin, *Noetherian operators and primary decomposition*, **arXiv:2006.13881** (2020).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

Towards a Theory of Domains for Harmonic Functions and its Symbolic Counterpart

***Bui Van Chien*[1]*, Gérard H.E. Duchamp*[2]*, Ngo Quoc Hoan*[3]*, V. Hoang Ngoc Minh*[4]**

[1] Hue University, 77, Nguyen Hue, Hue, Viet Nam,
bvchien.vn@gmail.com
[2]U niversité Paris Nord, 99, av. J-B Clément, 93430 Villetaneuse, France,
gerard.duchamp@lipn.univ-paris13.fr
[3] Hai Phong University, 171, Phan Dang Luu, Hai Phong, VietNam,
hoannq@dhhp.edu.vn
[4]University of Lille, 1, Place Déliot, 59024 Lille, France,
vincel.hoang-ngoc-minh@univ-lille.fr

In this talk, a sequel of [6], a theory of Domains for Harmonic Sums is proposed.

We begin by reviewing the calculus induced by the framework of [6]. In there, we extended Polylogarithm functions over a subalgebra of noncommutative rational power series, recognizable by finite state (multiplicity) automata over the alphabet $X = \{x_0, x_1\}$ (see [6]). The stability of this calculus under shuffle products relies on the nuclearity of the target space (see [17]). We also concentrated on algebraic and analytic aspects of this extension allowing to index polylogarithms, at non positive multi-indices, by rational series and also allowing to regularize divergent polyzetas, at non positive multi-indices (see [6]).

In this talk, as a continuation of works in [6] and in order to understand the bridge between the extension of this "polylogarithmic calculus" and the world of harmonic sums, we propose a local theory, adapted to a full calculus on indices of Harmonic Sums based on the Taylor expansions, around zero, of polylogarithms with index x_1 on the rightmost end. This theory is not only compatible with Stuffle products but also with the Analytic Model. In this respect, it provides a stable and fully algorithmic model for Harmonic calculus. Examples by computer are also provided.

Keywords
Generating series, Taylor expansion, Asymptotic expansion, Regularization.

References

[1]J. BERSTEL, C. REUTENAUER, *Rational series and their languages*, Spr.-Ver., 1988.
[2]J. BERSTEL, C. REUTENAUER, *Noncommutative Rational Series with Applications*, Encyclopedia of Mathematics and its Applications series, Cambridge University Press:248 pages, 2011.

[3] C. COSTERMANS; V. HOANG NGOC MINH, *Some Results à l'Abel Obtained by Use of Techniques à la Hopf*, Global Integrability of Field Theories and Applications, Daresbury, 2006.

[4] C. COSTERMANS; V. HOANG NGOC MINH, *Noncommutative algebra, multiple harmonic sums and applications in discrete probability*, Journal of Symbolic Computation, 801–817, 2009.

[5] BUI VAN CHIEN; V. HOANG NGOC MINH; NGO QUOC HOAN, *Families of eulerian functions involved in regularization of divergent polyzetas*, in preparation, 2020.

[6] G.H.E. DUCHAMP; V. HOANG NGOC MINH; NGO QUOC HOAN, *Kleene stars of the plane, polylogarithms and symmetries*, Theoretical Computer Science, (800):52–72, 2019.

[7] G.H.E. DUCHAMP; V. HOANG NGOC MINH; V. NGUYEN, *Towards a noncommutative Picard-Vessiot theory*, in preparation, 2020.

[8] B. V. DRINFRL'D, *On quasitriangular quasi-Hopf algebra and a group closely connected with* $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, Leningrad Math. J. , (4):829–860, 1991.

[9] J. HADAMARD, *Théorème sur les séries entières*, Acta Mathematica, 22:55– 63, 1899.

[10] V. HOANG NGOC MINH, *Summations of polylogarithms via evaluation transform*, Math. & Comput. Simul., 1336:707–728, 1996.

[11] V. HOANG NGOC MINH, *Differential Galois groups and noncommutative generating series of polylogarithms*, in Automata, Combinatorics and Geometry, 7th World Multiconference on Systemics, Cybernetics and Informatics, Florida, 2003.

[12] V. HOANG NGOC MINH, *Finite polyzêtas, Poly-Bernoulli numbers, identities of polyzêtas and noncommutative rational power series*, Proc. of 4th International Conference on Words, pages 232–250, 2003.

[13] V. HOANG NGOC MINH, *On the solutions of universal differential equation with three singularities*, Confluentes Mathematic, 11, no. 2:25–64, 2019.

[14] V. HOANG NGOC MINH; G. JACOB; N.E. OUSSOUS; M. PETITOT, *Aspects combinatoires des polylogarithmes et des sommes d'Euler-Zagier*, Journal électronique du Séminaire Lotharingien de Combinatoire, B43e, 2000.

[15] P. MONTEL, *Leons sur les familles normales de fonctions analytiques et leurs applications*, Gauthier-Villars, 2010.

[16] RICHARD P. STANLEY, *Enumerative Combinatorics*, Cambridge University Press, Vol. I, 1997.

[17] H. H. SCHAEFER AND M. P. WOLFF, *Topological Vector Spaces*, Springer-Verlag New York, 1999.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)”*

Factoring Difference Operators in Maple 2021.

Mark van Hoeij[1] [hoeij@math.fsu.edu]

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

The LREtools package in Maple 2021 contains algorithms I implemented for factoring difference operators. This talk gives an overview of these algorithms. Algorithm Minimal-Recurrence constructs a recurrence of proved minimal order for a sequence given by initial conditions and a (not necessarily minimal) recurrence. The degree-bound that is needed for the proof is constructed from asymptotic data computed by algorithm GeneralizedExponents. Algorithm RightFactors computes right-factors of recurrence operators. It contains two implementations. One implementation provably computes all (potentially infinitely many) right-factors of a specified order. The other is a fast heuristic that applies algorithm MinimalRecurrence to certain initial conditions. One application of these factoring implementations is algorithm SumDecompose, which can check if a solution of a recurrence can be written as sums of solutions of lower order recurrences, and if so, find such a decomposition. Factoring is also key to finding closed form solutions of higher order recurrence relations.

Keywords
Difference Operators, Factoring, Symbolic Computation.

References

[1] Y. CHA, M. VAN HOEIJ, G. LEVY, Solving Recurrence Relations using Local Invariants. *ISSAC'2010 Proceedings*, 2010.
[2] M. VAN HOEIJ, Factoring Linear Recurrence Operators. *slides of a presentation at Brasov Romania* www.math.fsu.edu/~hoeij/2019/slides.pdf 2019.
[3] Y. ZHOU, *PhD thesis in progress*, 2021.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)”*

Automatizing proofs of properties of operators

Clemens Hofstadler[1]***, Clemens G. Raab***[1]***, Georg Regensburger***[1] [clemens.hofstadler@jku.at]

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

Recently, two of the authors have developed a framework to rigorously prove statements about matrices and linear operators in a purely algebraic fashion [1]. To this end, operators are modelled as noncommutative polynomials and restrictions imposed by the domains and codomains of these operators are encoded in a labeled quiver. Then, proving that an identity of operators follows from other identities translates into verifying ideal membership of noncommutative polynomials and showing *compatibility* of certain polynomials with a quiver.

In this talk, we illustrate how this framework can be applied to problems in several different branches of mathematics. In particular, we discuss how to handle properties of operators that cannot be expressed in form of a single identity, such as quasi-identities or existential statements. For example, we show fully automated proofs of statements about Moore Penrose inverses as also published in [2] as well as of well-known theorems from homological algebra such as the five lemma. Furthermore, we present the MATHEMATICA package `OperatorGB` [3], which provides extensive support for proving properties of matrices and operators along the lines of the framework, and give a brief overview of the underlying algorithms implemented.

Keywords
matrices and linear operators, algebraic operator identities, automated proofs, noncommutative polynomials, quiver representations

References

[1] C. G. RAAB, G. REGENSBURGER, AND J. HOSSEIN POOR, Formal proofs of operator identities by a single formal computation. *J. Pure Appl. Algebra* **225**, Article 106564, 20 pages (2021).
[2] D. S. CVETKOVIĆ-ILIĆ, C. HOFSTADLER, J. HOSSEIN POOR, J. MILOŠEVIĆ, C. G. RAAB, AND G. REGENSBURGER, Algebraic proof methods for identities of matrices and operators: improvements of Hartwig’s triple reverse order law. *Appl. Math. Comput.*, to appear (2021).
[3] C. HOFSTADLER, Certifying operator identities and ideal membership of noncommutative polynomials. *Master’s thesis*, Johannes Kepler University Linz (2020).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

Multivariate Bernstein-type Polynomials of Finitely Generated D-Modules

Alexander Levin [levin@cua.edu]

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

In [1], I. Bernstein introduced an analog of the Hilbert polynomial for a finitely generated filtered module over a Weyl algebra $A_n(K)$, the ring of differential operators over the polynomial ring $K[x_1, \dots, x_n]$ generated by the partial derivations $\partial/\partial x_i$ $(1 \leq i \leq n)$. He also developed the theory of multiplicity for the class of such modules (called D-modules) and obtained interesting analytical applications of this theory (many of them are considered in Björk's book [2]).

In this presentation we prove the existence, determine invariants, and outline methods of computation of multivariate Bernstein-type polynomials of finitely generated D-modules associated with partitions of the basic sets of indeterminates and derivations. We show that such polynomials not only characterize the Bernstein class of left $A_n(K)$-modules, but also carry, in general, more invariants than the univariate Bernstein dimension polynomial. The presented results generalize the main results of [3] and give new properties of filtered D-modules and associated dimension polynomials.

Keywords
Weyl algebra, D-module, Dimension polynomial

References

[1] I. N. BERNSTEIN, Modules over the ring of differential operators. A study of the fundamental solutions of equations with constant coefficients. *Funct. Anal. and its Appl.* **5**, 89–101 (1971).
[2] J.-E. BJÖRK, *Rings of Differential Operators*. North Holland Publishing Co., Amsterdam, 1979.
[3] C. DÖNCH; A. LEVIN, Bivariate Dimension Polynomials and New Invariants of Finitely Generated D-modules. *Int. J. Algebra Comput.* **23** (7), 1625–1651 (2013).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

Commutative rings of Differential Operators

Emma Previato[1] [ep@math.bu.edu]

[1] Department of Mathematics and Statistics, Boston University, Boston, MA, USA

Maximal-commutative algebras of ordinary differential operators (ODOs), equivalently, centralizers of a given ODO, are a topic of current interest and many open problems. The notion of rank plays a major role. In the Weyl algebra W, namely ODOs with polynomial coefficients, the problems become more difficult. This talk will review the Dixmier test [1] and present its computational implementation [3] in W, for the case study of centralizers of 4th order ODOs. The algorithm, automated in Maple 18, starts with an ODO L of order 4 (in normalized form) and, provided the centralizer is non-trivial, by iterating the division algorithm finds a commuting operator B such that the pair $L,\ B$ is a basis of the centralizer as module over the polynomial ring in one variable; it also yields the equation of the spectral curve of the centralizer and an explicit presentation of the rank-2 vector bundle consisting of common eigenfunctions, via (sub)resultants. The theory is based on the algebro-geometric interpretation of the objects of study in terms of the spectral curve. Klein's quartic curve is not capable of such an interpretation, and a generalization of the theory is devised, that produces commutative rings of matrix ODOs (cf. [2]). We then pursue the study of commutative rings of matrix ODOs with polynomial coefficients. This is work in collaboration with Sonia L. Rueda and Maria-Angeles Zurro.

Keywords
Weyl Algebra, Rank of an Algebra of Differential Operators, Klein Quartic Curve

References

[1] J. DIXMIER, Sur les algèbres de Weyl. *Bull. Soc. Math. France* **96**, 209–242 (1968).
[2] I.M. KRICHEVER, Algebraic curves and commuting matrix differential operators. *Funkcional. Anal. i Priložen.* **10**(2), 75–76 (1976).
[3] E. PREVIATO; S.L. RUEDA; M.-A. ZURRO, Commuting ordinary differential operators and the Dixmier test. *SIGMA Symmetry Integrability Geom. Methods Appl.* **15**(Paper No. 101), 23 pp. (2019).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)”*

Factoring Third Order Ordinary Differential Operators over Spectral Curves

Sonia L. Rueda[1]***, Maria-Angeles Zurro***[2] [sonialuisa.rueda@upm.es]

[1] Dpto. de Matemática Aplicada. Universidad Politécnica de Madrid. Spain
[2] Dpto. de Matemáticas. Universidad Autónoma de Madrid. Spain

We consider the factorization problem of a third order ordinary differential operator $L - \lambda$, for a spectral parameter λ and an irreducible operator L, whose coefficients belong to a differential field K. It is assumed that L is algebro-geometric over K, guarantying a nontrivial centralizer, which can be seen as the ring of an affine curve, the famous *spectral curve* Γ.

Based on the nature of Γ, we give a symbolic algorithm to factor $L - \lambda$ over the spectral curve using differential subresultants. In this context, the first explicit example of a non-planar spectral curve arises, as well as the factorization it provides for $L - \lambda$. As far as we know, it is the first factorization algorithm for third order irreducible operators over the field extension $K(\Gamma)$ of K. The coefficient field K is extended to the field of rational functions on Γ to obtain a right factor with coefficients in this field.

Factorizations over planar spectral curves have been presented in other articles, for instance for second order operators [1], or fourth order operators with rank 2, [3]. The present work is the natural continuation in a program dedicated to the factorization of rank 1 algebro-geometric differential operators, that was already successful in the order 2 case, [1]. Our ultimate goal is an effective approach to the direct spectral problem and the development of the appropriate *spectral Picard-Vessiot fields* containing all the solutions of the operator $L - \lambda$. Spectral Picard-Vessiot fields were studied for Schrödinger operators in [2].

Keywords
Factorization, ordinary differential operators, differential subresultant, spectral curve.

References

[1] J.J. Morales-Ruiz. S.L. Rueda, and M.A. Zurro. *Factorization of KdV Schrödinger operators using differential subresultants*. Adv. Appl. Math., 120:102065, 2020.

[2] J.J. Morales-Ruiz. S.L. Rueda, and M.A. Zurro. *Spectral Picard-Vessiot fields for algebro-geometric Schrödinger operators* . To appear in Ann. Inst. Fourier. Arxiv https://arxiv.org/abs/1708.00431, 2021.

[3] E. Previato, S.L. Rueda, and M.A. Zurro. *Commuting Ordinary Differential Operators and the Dixmier Test*. SIGMA Symmetry Integrability Geom. Methods Appl., 15(101):23 pp., 2019.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

Integral bases of P-recursive operators

Shaoshi Chen[2,3]***, Lixin Du***[1,2,3]***, Manuel Kauers***[1]***, Thibaut Verron***[1] [thibaut.verron@jku.at]

[1] Institute for Algebra, Johannes Kepler University, Linz, Austria
[2] KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China
[3] School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing, China

Integral bases are a central concept when studying algebraic field extensions, with applications including the computation of short generators or symbolic integration [2]. In recent work [1], similar bases were defined over differential Ore algebras. They can be computed with a generalization of an algorithm from the algebraic case [3], and they have the same application to the computation of integrals.

In this work, we explain how to extend the definition and the construction to other Ore algebras, such as those defined with a "shift" operator. More generally, we extend the definition to valued vector spaces satisfying some additional axioms. This setting contains the known cases of algebraic extensions and differential Ore algebras, and we show that shift Ore algebras can be equipped with a suitable valuation. As a result, we obtain a general framework for defining and computing integral bases.

Keywords
Ore algebra, Shift operators, integral bases

References

[1] S. CHEN; M. VAN HOEIJ; M. KAUERS; C. KOUTSCHAN, Reduction-based creative telescoping for Fuchsian D-finite functions. *Journal of Symbolic Computation* **85**, 108–127 (2018).
[2] B. M. TRAGER, *Integration of Algebraic Functions*. PhD thesis, MIT, 1984
[3] M. VAN HOEIJ, An algorithm for computing an integral basis in an algebraic function field. *Journal of Symbolic Computation* **18**(4), 353–363 (1994)

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)”*

On sequences associated to the invariant theory of rank two simple Lie algebras

***Alin Bostan*[1]*, Jordan Tirrell*[2]*, Bruce W. Westbury*[3]*, Yi Zhang*[4]** [Yi.Zhang03@xjtlu.edu.cn]

[1] Inria, Université Paris-Saclay, 1 rue Honoré d’Estienne d’Orves, 91120 Palaiseau, France
[2] Department of Mathematics and Computer Science, Washington College, USA
[3] Department of Mathematical Sciences, The Unversity of Texas at Dallas, USA
[4] Department of Applied Mathematics, School of Science, Xi’an Jiaotong-Liverpool University, Suzhou, 215123, China

The representation theory of simple Lie algebras is a cornerstone of algebraic and enumerative combinatorics, giving rise to combinatorial objects such as tableaux, symmetric functions, quantum groups, crystal graphs, and so on. We are interested in two families of sequences in OEIS. Sequences in the first family of sequences are called *octant sequences*. For example, sequence A059710, which is the first octant sequence, is defined to be a sequence associated to fundamental representations of the exceptional simple Lie algebra G_2, of rank two and dimension fourteen [4]. The second octant sequence is A108307 [5], and it is defined to be the cardinality of the set of set partitions of $[n]$ with no enhanced 3-crossing. Our first contribution is to prove that sequences A059710 and A108307 are tightly related by a binomial transform.

Theorem 0.1. *Let $T_3(n)$ and $E_3(n)$ be the n-th terms of A059710 and A108307, respectively. Then E_3 is the binomial transform of T_3, , for $n \geq 0$,*

$$E_3(n) = \sum_{k=0}^{n} \binom{n}{k} T_3(k).$$

Theorem 0.1 provides an unexpected connection between invariant theory of G_2 and combinatorics of set partitions. In the same spirit, [5] and [3] prove a binomial relation between E_3 and A108304, which is the third octant sequence, respectively. In summary, these two results show that the octant sequences are associated to representations of G_2.

Based on Theorem 0.1, as well as on results by Bousquet-Mélou and Xin [1], our second contribution is to give two independent proofs of a recurrence equation for T_3 conjectured by Mihailovs [6], which was the initial motivation for our study:

Theorem 0.2. *The sequence T_3 is determined by the initial conditions $T_3(0) = 1$, $T_3(1) = 0$, $T_3(2) = 1$ and the recurrence relation that for $n \geq 0$,*

$$\begin{aligned}14(n+1)(n+2)T_3(n) + (n+2)(19n+75)T_3(n+1) \\ + 2(n+2)(2n+11)T_3(n+2) - (n+8)(n+9)T_3(n+3) = 0. \quad (1)\end{aligned}$$

Moreover, we give an alternative proof of Theorem 0.2, using the interpretation of T_3 in terms of G_2 walks and using algorithms for computing Picard-Fuchs differential equations for algebraic residues. As a consequence, closed formulae for the generating function of T_3 are obtained in terms of the classical Gaussian hypergeometric function.

We consider a second family of sequences, called *quadrant sequences*. These are defined to be sequences associated to representations of G_2 restricted to $SL(3)$. By invariant theory, these sequences are also are related by binomial transforms. Based on this, we derive a uniform recurrence equation holding *for each quadrant sequence*. Furthermore, we show that sequences in the second family are identical to quadrant sequences because they satisfy the same initial conditions and recurrence equations. They are related to the octant sequences by the branching rules [1] for the maximal subgroup $SL(3)$ of G_2.

Keywords
representation theory, binomial transforms, recurrence equations

References

[1] M. Bousquet-Mélou; G. Xin, On partitions avoiding 3-crossings. *Sém. Lothar. Combin..* **21**(54), Art. B54e (2005).
[2] R. Gaskell; R. T. Sharp, Generating functions for G_2 characters and subgroup branching rules. *J. Math. Phys.* **22**(12), 2736–2739 (1981).
[3] J. B. Gil; J. O. Tirrell, A simple bijection for enhanced, classical, and 2-distant k-noncrossing partitions. *Disc. Math.*, **343**(6), 111705 (2020)
[4] G. Kuperberg, Spiders for rank 2 Lie algebras. *Comm. Math. Phys.*, **180**(1), 109–151 (1996)
[5] Z. Lin, Restricted inversion sequences and enhanced 3-noncrossing partitions. *European J. Combin..*, **70**, 202–211 (2018)
[6] B. W. Westbury, Enumeration of non-positive planar trivalent graphs. *J. Algebraic Combin.*, **25**(4), 357–373 (2007)

S13. Algorithmic Combinatorics

Organized by

Hao Du, Christoph Koutschan and Ali Uncu

Applications of Computer Algebra - ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Algorithmic Combinatorics*

The DEWCAD Project: Pushing Back the Doubly Exponential Wall of Cylindrical Algebraic Decomposition

Russell Bradford*[1]*, James H. Davenport*[1]*, Matthew England*[2]*, Amirhossein Sadeghimanesh*[2]*,
Ali K. Uncu[1] [aku21@bath.ac.uk]

[1] University of Bath, Faculty of Science, Department of Computer Science, Bath, BA2 7AY, UK
[2] Coventry University, Faculty of Engineering, Department of Computer Science, Coventry, CV1 2JH, UK

Cylindrical Algebraic Decomposition (CAD), was developed by Collins in the 1970s. Originally it was introduced to perform quantifier elimination over reals; given a formula with some quantifiers on variables, CAD finds an equivalent form without quantifiers. However, CAD should really be considered as a general tool for working with subsets of $\mathbb{R}^n$ that can be described by polynomial equations and inequalities. It can be used in deciding the correctness, satisfiability, and various other properties of a given set of polynomial constraints (possibly with quantified variables). CAD has many applications in combinatorics and other research fields and good implementations of it is in high demand.

This presentation aims to introduce the ACA community to the DEWCAD project, which is based at Coventry University and the University of Bath, in the United Kingdom. The project seeks to push back the Doubly Exponential Wall of Cylindrical Algebraic Decomposition, through the integration of SAT/SMT technology, the extension of Lazard projection theory, and the development of new algorithms based on CAD technology but without producing CADs themselves. The project also seeks to develop more applications of CAD to various fields.

Keywords
Cylindric Algebraic Decomposition

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Algorithmic Combinatorics*

Rational Ehrhart Theory

Matthias Beck[1,2]***, Sophia Elia***[1] ***and Sophie Rehberg***[1] [mattbeck@sfsu.edu]

[1] Mathematisches Institut, Freie Universität Berlin, Germany
[2] Department of Mathematics, San Francisco State University, U.S.A.

The Ehrhart quasipolynomial of a rational polytope P encodes fundamental arithmetic data of P, namely, the number of integer lattice points in positive integral dilates of P. Ehrhart quasipolynomials were introduced in the 1960s, satisfy several fundamental structural results and have applications in many areas of mathematics and beyond. The enumerative theory of lattice points in rational (equivalently, real) dilates of rational polytopes is much younger, starting with work by Linke [1], Baldoni–Berline–Koeppe–Vergne [2], and Stapledon [3]. We introduce a generating-function *ansatz* for rational Ehrhart quasipolynomials, which unifies several known results with classical Ehrhart quasipolynomials, as well as generalized reflexive polytopes studied by Fiset–Kasprzyk [4] and Kasprzyk–Nill [5].

Keywords
rational polytope, lattice point enumeration, rational Ehrhart quasipolynomial

References

[1] EVA LINKE, Rational Ehrhart quasi-polynomials. *J. Combin. Theory Ser. A* **118**(7), 1966–1978 (2011).
[2] VELLEDA BALDONI, NICOLE BERLINE, MATTHIAS KÖPPE, AND MICHÈLE VERGNE, Intermediate sums on polyhedra: computation and real Ehrhart theory. *Mathematika* **59**(1), 1–22 (2013).
[3] ALAN STAPLEDON, Counting lattice points in free sums of polytopes. *J. Combin. Theory Ser. A* **151**, 51–60 (2017).
[4] MATTHEW H. J. FISET AND ALEXANDER M. KASPRZYK, A note on palindromic δ-vectors for certain rational polytopes. *Electron. J. Combin.* **15**(1), Note 18, 4 pp. (2008).
[5] ALEXANDER M. KASPRZYK AND BENJAMIN NILL, Reflexive polytopes of higher index and the number 12. *Electron. J. Combin.* **19**(3), Paper 9, 18 pp. (2012).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Algorithmic Combinatorics*

Separability Problems in Creative Telescoping

Shaoshi Chen[1], ***Ruyong Feng***[1,2], ***Pingchuan Ma***[1,2], ***and Michael F. Singer***[3]
[schen@amss.ac.cn]

[1] KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, 100190, China
[2] School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China
[3] Department of Mathematics, North Carolina State University, Raleigh, NC 27695, USA

For given multivariate functions specified by algebraic, differential or difference equations, the separability problem is to decide whether they satisfy linear differential or difference equations in one variable. In this talk, we will explain how separability problems arise naturally in creative telescoping and present some criteria for testing the separability for several classes of special functions, including rational functions, hyperexponential functions, hypergeometric terms, and algebraic functions.

Keywords
Creative telescoping, Separable functions, Separation of variables, Zeilberger's algorithm

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Algorithmic Combinatorics*

Constructing minimal telescopers for rational functions in three discrete variables *

Shaoshi Chen[1], ***Qing-Hu Hou***[2], ***Hui Huang***[3], ***George Labahn***[4], ***Rong-Hua Wang***[5]
[huanghui@dlut.edu.cn]

[1] KLMM, AMSS, Chinese Academy of Sciences, Beijing, China
[2] Center for Applied Mathematics, Tianjin University, Tianjin, China
[3] School of Mathematical Sciences, Dalian University of Technology, Dalian, China
[4] Symbolic Computation Group, University of Waterloo, Waterloo, Canada
[5] School of Mathematical Sciences, Tianjin Polytechnic University, Tianjin, China

Creative telescoping is a powerful method pioneered by Zeilberger [5, 6] in the 1990s and has now become the cornerstone for finding closed forms for definite sums (and definite integrals) in computer algebra. In the case of summation, specialized to the trivariate case, in order to compute a sum of the form $\sum_{y=a_1}^{b_1} \sum_{z=a_2}^{b_2} f(x,y,z)$, the main task of creative telescoping consists in finding rational functions (or polynomials) $c_0, \ldots, c_\rho$ in x, not all zero, and two functions $g(x,y,z), h(x,y,z)$ in the same domain as f such that

$$\begin{aligned} & c_0(x) f(x,y,z) + c_1(x) f(x+1,y,z) + \cdots + c_\rho(x) f(x+\rho,y,z) \\ &= g(x,y+1,z) - g(x,y,z) + h(x,y,z+1) - h(x,y,z). \end{aligned} \tag{1}$$

We call the nonzero operator $L = c_\rho S_x^\rho + \cdots + c_1 S_x + c_0$ with S_x being the shift operator in x a *telescoper* for f and the pair (g,h) a *certificate* for L.

Various algorithmic generalizations and improvements for the method of creative telescoping have been developed over the past two decades. At the present time, the reduction-based approach has gained the most support as it is both efficient in practice and has the important feature of being flexible to find a telescoper for a given special function with or without construction of a certificate. This is desirable in the typical situation where only the telescoper is of interest and its size is much smaller than that of the certificate.

In this talk, we describe a recent algorithm developed by the authors in [2] for constructing minimal telescopers for rational functions in three discrete variables. This is the first step toward developing reduction-based creative telescoping algorithms for special functions having more than two discrete variables.

*S. Chen was supported by the NSFC grants 11501552, 11871067, 11688101 and by the Frontier Key Project (QYZDJ-SSW-SYS022) and the Fund of the Youth Innovation Promotion Association, CAS. Q. Hou was supported by the NSFC grant 11771330. H. Huang was supported by the Fundamental Research Funds for the Central Universities. G. Labahn was supported by the NSERC RGPIN-2020-04276 Canada. R. Wang was supported by the NSFC grants 11871067 and 11626170.

As with other reduction-based algorithms, our starting point is to find a suitable reduction for trivariate rational functions. In particular, based on Hou and Wang's work in [4], along with the use of difference homomorphisms, we extend the Abramov reduction [1] for determining summability of univariate rational functions to bivariate ones. This extended reduction brings the given rational function $f(x, y, z)$ to another rational function $\mathrm{red}(f)$ modulo summable ones, namely rational functions admitting the form as the right-hand side of (1), where $\mathrm{red}(f)$ satisfies: (i) $\mathrm{red}(f) = 0$ whenever f is summable, and (ii) $\mathrm{red}(f)$ is minimal in certain sense. Such a $\mathrm{red}(f)$ is unique up to congruence modulo summable rational functions. In order to find a telescoper for f, we then iteratively compute $\mathrm{red}(f), \mathrm{red}(S_x(f)), \mathrm{red}(S_x^2(f)), \ldots$ until we find rational functions $c_0, \ldots, c_\rho$ in x, not all zero, such that

$$c_0 \,\mathrm{red}(f) + \cdots + c_\rho \,\mathrm{red}(S_x^\rho(f)) \equiv 0 \mod (\text{summable rational functions}).$$

By showing that the expression on the left-hand side is congruent to $\mathrm{red}(c_0 f + \cdots + c_\rho S_x^\rho(f))$, we conclude from the minimality of $\mathrm{red}(\cdot)$ that $\mathrm{red}(c_0 f + \cdots + c_\rho S_x^\rho(f)) = 0$. This thus implies that $c_0 f + \cdots + c_\rho S_x^\rho(f)$ is summable, yielding a telescoper $c_0 + \cdots + c_\rho S_x^\rho$ for f. Note that the first nontrivial linear dependency leads to a telelscoper of minimal order, and the termination of our algorithm is guaranteed by a known existence criterion of telescopers developed in [3].

One can tell from the above description that our algorithm finds a minimal telescoper for a given trivariate rational function without also needing to compute an associated certificate. Computational experiments will be provided so as to illustrate the efficiency of our algorithm.

Keywords
Abramov reduction, Telescoper, Difference homomorphism

References

[1] S. A. ABRAMOV, The rational component of the solution of a first-order linear recurrence relation with a rational right side. *USSR Comput. Math. Math. Phys.* **15**(4), 216–221 (1975).
[2] S. CHEN; Q.-H. HOU; H. HUANG; G. LABAHN; R.-H. WANG, Constructing minimal telescopers for rational functions in three discrete variables. *Preprint: arXiv:1904.11614*.
[3] S. CHEN; Q.-H. HOU; G. LABAHN; R.-H. WANG, Existence problem of telescopers: beyond the bivariate case. In *Proceedings of ISSAC'16*, Markus Rosenkranz (eds.), 167–174. ACM, New York, 2016.
[4] Q.-H. HOU; R.-H. WANG, An algorithm for deciding the summability of bivariate rational functions. *Adv. in Appl. Math.* **64**, 31–49 (2015).
[5] D. ZEILBERGER, A holonomic systems approach to special functions identities. *J. Comput. Appl. Math.* **32**(3), 321–368 (1990).
[6] D. ZEILBERGER. The method of creative telescoping. *J. Symbolic Comput.* **11**(3), 195–204 (1991).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Algorithmic Combinatorics*

Quadrant Walks Starting Outside the Quadrant

Manual Kauers[1]***, Manfred Buchacher***[1] ***and Amelie Trotignon***[1] [manuel@kauers.de]

[1] Institute for Algebra, Johannes Kepler University (JKU), Altenberger Straße 69, 4040 Linz, Austria

We investigate a functional equation which resembles the functional equation for the generating function of a lattice walk model for the quarter plane. The interesting feature of this equation is that its orbit sum is zero while its solution is not algebraic. The solution can be interpreted as the generating function of lattice walks in $\mathbb{Z}^2$ starting at $(-1,-1)$ and subject to the restriction that the coordinate axes can be crossed only in one direction. We also consider certain variants of the equation, all of which seem to have transcendental solutions. In one case, the solution is perhaps not even D-finite.

Keywords
Lattice Walks, Kernel Method, D-finite functions, Transcendence

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Algorithmic Combinatorics*

A combinatorial construction for two formulas in Slater's List

Kağan Kurşungöz[1] [kursungoz@sabanciuniv.edu]

[1] Faculty of Engineering and Natural Sciences, Sabancı University, İstanbul, Turkey

Number 19 in Slater's list [4] is

$$(-q;q)_\infty \sum_{n\geq 0} \frac{(-1)^n q^{3n^2}}{(q^2;q^2)_n (-q;q)_{2n}} = \frac{1}{(q;q^5)_\infty (q^4;q^5)_\infty},$$

where we use the q-Pochhammer symbols

$$(a,q)_n := \prod_{j=1}^{n} (1-aq^{n-1}), \quad (a,q)_\infty = \lim_{n\to\infty} (a,q)_n.$$

We set up a combinatorial framework for inclusion-exclusion on the partitions into distinct parts to obtain the same series as an alternative generating function of partitions into distinct and non-consecutive parts. In connection with Rogers-Ramanujan identities, the generating function yields the aforementioned formula in Slater's list, along with its sister, namely number 15. The same formulas were constructed by Hirschhorn [2]. Similar formulas were obtained by Bringmann, Mahlburg and Nataraj [1]. These are part of the results in [3].

Keywords
integer partition, partition generating function, Rogers-Ramanujan identities, Slater's list

References
[1] K. Bringmann, K. Mahlburg, K. Nataraj, Distinct parts partitions without sequences, *The Electronic Journal of Combinatorics*, **22**(3), (2015), #P3.3.
[2] M.D. Hirschhorn, *Developments in the Theory of Partitions*, Ph.D. thesis, University of New South Wales (1979).
[3] K. Kurşungöz, A combinatorial construction for two formulas in Slater's list. *International Journal of Number Theory*, **17**(03), 655–663 (2021).
[4] L. J. Slater, Further Identities of the Rogers-Ramanujan Type, *Proc. London Math. Soc. Ser. 2* **54**, 147–167 (1952).

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

Enumerative Properties of Cogrowth Series on Free Products of Finite Groups

Jason Bell[1], ***Haggai Liu***[2], ***Marni Mishna***[2] [haggail@sfu.ca]

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

Given a group G with a finite set of generators, S, it is natural to ask if the product of n generators from S evaluate to the identity. The enumerative version of this problem, known as the *cogrowth* problem, counts the number of such products and studies the associated counting sequence. Many cogrowth sequences are known. We focus on the free products of finite groups: Specifically, cyclic and dihedral groups. Such groups have the property that their cogrowth generating functions are algebraic functions, and thus, are solutions to implicit polynomial equations. Using algebraic elimination techniques and free probability theory, we establish upper bounds on the degrees of the polynomial equations that they satisfy. This has implications for asymptotic enumeration, and makes it theoretically possible to determine the functions explicitly.

Keywords
cogrowth, polynomial, algebraic, series, generating function

References

[1] J BELL; M MISHNA, On the Complexity of the Cogrowth Sequence. *arXiv* **1805.08118v1**, (2018).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Algorithmic Combinatorics*

Combinatorial Exploration: A New Approach to Enumeration

Michael Albert*[1]*, Christian Bean*[2]*, Anders Claesson*[3]*, Émile Nadeau*[2]*, Jay Pantone*[4]*, Henning Ulfarsson*[2]*, [jay.pantone@marquette.edu]

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

Combinatorial structures are ubiquitous throughout mathematics. Graphs, permutations, words, and other such families of combinatorial objects often play a central role in work from many different fields. The study of enumerative combinatorics is concerned with the elucidation of structural properties of these families, including counting, classification, and limiting behavior.

Combinatorial Exploration is a framework that unifies the often ad-hoc methods used in enumerative combinatorics. In this talk we'll explain how Combinatorial Exploration works, how it can be automated, and how it's being applied to the study of pattern-avoiding permutations to prove new results and reprove dozens of old ones.

Keywords
Enumeration, Automatic, Experimental

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23–27, 2021
Session on *Algorithmic Combinatorics*

The size of the minimal automaton for an algebraic sequence

Eric Rowland[1]***, Manon Stipulanti***[2]***, Reem Yassawi***[3] [eric.rowland@hofstra.edu]

[1] Department of Mathematics, Hofstra University, Hempstead, NY, USA
[2] Department of Mathematics, University of Liège, Liège, Belgium
[3] School of Mathematics and Statistics, Open University, Milton Keynes, UK

Let $s(n)_{n\geq 0}$ be a sequence whose terms are elements of a finite field $\mathbb{F}_q$. A major theorem of Christol [2, 3] states that $s(n)_{n\geq 0}$ is algebraic if and only if it is q-automatic. That is, there exists a nonzero polynomial $P(x,y) \in \mathbb{F}_q[x,y]$ such that $P(x, \sum_{n\geq 0} s(n)x^n) = 0$ if and only if there is a finite automaton that outputs $s(n)$ when fed the base-q digits of n (say, starting with the least significant digit).

We therefore have two quite different ways of representing q-automatic sequences — polynomials and automata. A natural question is how the size of the minimal polynomial for a sequence (measured by its x-degree and y-degree) relates to the size of the minimal automaton for the sequence (measured by the number of states), and vice versa.

Given an algebraic series $\sum_{n\geq 0} s(n)x^n$ specified by a polynomial $P(x,y)$ with x-degree h, y-degree d, and genus g, Bridy [1] used algebraic geometry techniques to obtain the upper bound $(1+o(1))q^{h+d+g-1}$ on the number of states in the minimal automaton generating $s(n)_{n\geq 0}$, where $o(1)$ tends to 0 as any of q, h, d, g gets large.

We show that progress can be made toward this bound without using tools from algebraic geometry, by analyzing orbits of certain linear operators on a finite-dimensional vector space of bivariate polynomials.

Keywords
automatic sequence, algebraic sequence, Christol's theorem

References

[1] A. Bridy, Automatic sequences and curves over finite fields, *Algebra & Number Theory* **11**, 685–712 (2017).
[2] G. Christol, Ensembles presque periodiques k-reconnaissables, *Theoretical Computer Science* **9**, 141–145 (1979).
[3] G. Christol, T. Kamae, M. Mendès France, and G. Rauzy, Suites algébriques, automates et substitutions, *Bulletin de la Société Mathématique de France* **108**, 401–419 (1980).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Algorithmic Combinatorics*

Binomial Determinants for Tiling Problems Yield to the Holonomic Ansatz

***Hao Du*[1]*, Christoph Koutschan*[2]*, Thotsaporn Thanatipanonda*[3] *and Elaine Wong*[2]**
[elaine.wong@ricam.oeaw.ac.at]

[1] School of Sciences, Beijing University of Posts and Telecommunications (BUPT), Beijing 100876, China
[2] Johann Radon Institute (RICAM), Austrian Academy of Sciences, Altenberger Straße 69, 4040 Linz, Austria
[3] Science Division, Mahidol University International College (MUIC), Nakhonpathom, 73170, Thailand

We present and prove closed form expressions for some families of binomial determinants with signed Kronecker deltas that are located along an arbitrary diagonal in the corresponding matrix. They count cyclically symmetric rhombus tilings of hexagonal regions with triangular holes. We extend a previous systematic study of these families, where the locations of the Kronecker deltas depended on an additional parameter, to families with negative Kronecker deltas. By adapting Zeilberger's holonomic ansatz to make it work for our problems, we can take full advantage of computer algebra tools for symbolic summation. This, together with the combinatorial interpretation, allows us to realize some new determinantal relationships. From there, we are able to resolve all remaining open conjectures related to these determinants, including one from 2005 due to Lascoux and Krattenthaler.

Keywords
Binomial determinant, Creative telescoping, Holonomic ansatz, Rhombus tiling, Non-intersecting lattice paths, Symbolic summation

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Algorithmic Combinatorics*

Combinatorics of Truncated Partition Theorems

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

[1] Mathematics Department, The Pennsylvania State University, University Park, PA 16802, USA

In 2012, Andrews and Merca derived a truncated version of Euler's pentagonal number theorem, which yields the following partition inequalities: For $k \geq 1$ and $n \geq 1$,

$$(-1)^{k-1}\sum_{j=0}^{k-1}(-1)^j\left(p\left(n-\frac{j(3j+1)}{2}\right)-p\left(n-\frac{(j+1)(3j+2)}{2}\right)\right)\geq 0,$$

where $p(N)$ denotes the partition function.

The work of Andrews and Merca has opened up a new study on truncated theta series inspiring several mathematicians to work on truncated theta series. In this study, analytic and combinatorial methods have been equally instrumental, but it seems hard to identify any common thread that runs through all existing combinatorial proofs. Recently, Ernest Xia and Xiang Zhao found several new identities on truncated series, which motivated me to study the whole phenomenon from a combinatorial point of view. In this talk, I will present some ideas and progress.

Keywords
Integer partitions, overpartitions, pod partitions, theta series, truncated series

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Algorithmic Combinatorics*

Diagonals and hypergeometric functions

Sergey Yurkevich[1]**, *Alin Bostan***[2] [sergey.yurkevich@univie.ac.at]

[1] University of Vienna, Austria
[2] Inria, Université Paris-Saclay, France

The diagonal of a multivariate power series $g = \sum_{i_1,\dots,i_n} g_{i_1,\dots,i_n} x_1^{i_1} \cdots x_n^{i_n} \in \mathbb{Q}[\![x_1,\dots,x_n]\!]$ is defined as the univariate series $\mathrm{Diag}(g) = \sum_{j \geq 0} g_{j,\dots,j} t^j \in \mathbb{Q}[\![t]\!]$. Diagonals not only have intriguing intrinsic properties, but also play an important role in combinatorics, in the study of special functions and even in physics. Although much is known about them, fundamental conjectures surprisingly remain open. In this talk we are interested in the following unsolved (dual) questions:

(i) What are the rational series $g(x_1,\dots,x_n)$ whose diagonal is a power series of a sequence following a first order linear recursion, i.e $\mathrm{Diag}(g)$ is a generalized hypergeometric function ${}_pF_q$?

(ii) What are the hypergeometric sequences $(a_j)_{j\geq 0}$ whose generating functions $\sum_{j\geq 0} a_j t^j$ can be written as diagonals of rational power series?

While (i) is known to be algorithmically decidable, the status of (ii) is still famously unclear: for example, Christol's old but still open problem is to decide whether the function ${}_3F_2([1/9, 4/9, 5/9], [1/3, 1], t)$ can be written as the diagonal of a rational series.

Recently, Abdelaziz, Koutschan and Maillard [1], and shortly later Bostan and the speaker [2] achieved progress on the questions (i) and (ii). The talk will explain the main ideas, methods and difficulties of the approaches. It will provide more insight in the algorithmic and experimental nuances of the main results.

Keywords
Hypergeometric functions, Diagonals, Christol's conjecture

References

[1] Y. ABDELAZIZ, C. KOUTSCHAN, J-M. MAILLARD, On Christol's conjecture. *Journal of Physics A: Mathematical and Theoretical* **53**(20), (2020).
[2] A. BOSTAN, S. YURKEVICH, On a class of hypergeometric diagonals. To appear in *Proceedings of the American Mathematical Society*.

S14. Algorithms for Polynomial System Solving and their Applications

Organized by

Ryoya Fukasaku, Yosuke Sato and Tateaki Sasaki

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Session Title"*

Comprehensive Gröbner systems in CoCoA

Elisa Palezzato[1]***, Anna M. Bigatti***[2]***, Michele Torielli***[3] [palezzato@math.sci.hokudai.ac.jp]

[1] Department of Mathematics, Hokkaido University, Sapporo, Japan
[2] Department of Mathematics, University of Genova, Genova, Italy
[3] Department of Mathematics, GI-CoRE GSB, Hokkaido University, Sapporo, Japan

1 Comprehensive Gröbner systems

The concepts of a comprehensive Gröbner system (CGS) was introduced by Weispfenning [6] to associate Gröbner basis like objects for parametric polynomial systems. For a specialization of parameters, a Gröbner basis of the specialized ideal can be immediately recovered from a branch of the associated CGS. This property of CGS make them attractive in applications where a family of related problems can be parameterized and specified using a parametric polynomial system.

Several improvements have been done by Weispfenning (CCGB [7]), Montes (DISPGB [3]) and Suzuki-Sato (ACGB [4]). However, all these algorithms essentially require computations in polynomial ring over a coefficient field of rational functions, $K(A)[X]$, where K is the ground field and A are the parameters and X the actual indeterminates, together with delicate handling the case distinctions over the parameters. This last fact makes these algorithms hard to implement in computer algebra systems.

In 2006 Suzuki-Sato [5] introduced a new approach to compute comprehensive Gröbner systems and comprehensive Gröbner bases. Making good use of some results by Kalkbrener [2], their algorithms do not require case distinctions to be pairwise disjoint and just need the final result of Gröbner bases in $K[A, X]$, so that that can be easily implemented in any computer algebra system. Suzuki and Sato implemented their algorithms in several computer algebra systems such as Risa/Asir, Singular and Maple and proved that it is sufficiently fast comparing with existing implementations when there are few parameters.

This approach attracted our attention and we decided to implement their algorithm also in the computer algebra system CoCoA [1]. We designed some optimization and made comparisons, and we wish to present and discuss our work in progress.

Keywords
Comprehensive Gröbner systems, Gröbner bases, CoCoA

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] K. KALKBRENER, *On the stability of Gröbner bases under specialization*, J. Symb. Comp. 24(1), 51–58 (1997).

[3] M. MANUBENS; A. MONTES, *Improving the DISPGB algorithm using the discriminant ideal*. J. Symb. Comp. 41(11), 1245–1263 (2006).

[4] A. SUZUKI; Y. SATO, *An Alternative approach to Comprehensive Gröbner Bases*. J. Symb. Comp. 36(3-4), 649–667 (2003).

[5] A. SUZUKI; Y. SATO, *A Simple Algorithm to Compute Comprehensive Gröbner Bases Using Gröbner Bases*. ISSAC '06: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation, 326–331, 2006.

[6] V. WEISPFENNING, *Comprehensive Gröbner bases*, J. Symb. Comp. 14(1), 1–29 (1992).

[7] V. WEISPFENNING, *Canonical Comprehensive Gröbner bases*, J. Symb. Comp. 36, 669–683 (2003).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Algorithms for Polynomial System Solving and Their Applications'*

Double Ideal Quotient and Its Applications

Yuki Ishihara[1] [yishihara@rs.tus.ac.jp]

[1] Department of Applied Mathematics, Tokyo University of Science, Tokyo, Japan

We introduce a special ideal operation "Double Ideal Quotient (DIQ)" and its variants, which are very useful tools for localizations of ideals. For ideals I and J in the n-variables polynomial ring $K[X] = K[x_1, \dots, x_n]$ over a field K, we call $(I : (I : J))$ the *double ideal quotient* of I and J. Replacing such ideal quotients by saturations, we can consider its variants; $(I : (I : J)^\infty)$, $(I : (I : J^\infty)^\infty)$ and $(I : (I : J^\infty))$. DIQ and its variants have many properties on primary components and prime divisors; for example, they give us

- Criteria for prime divisors
- Criteria for primary components
- Criteria for isolated (embedded) prime divisors
- A way to compute equidimensional hulls
- A way to compute pseudo-primary components from given prime divisors
- A way to compute (isolated) primary components from given (isolated) prime divisors

We explain some details. First, we have the following criterion for prime divisors.

Proposition 1 ([5], Corollary 3.4)**.** *Let I be an ideal and P a prime ideal. Then, P is a prime divisor of I if and only if $P \supset (I : (I : P))$.*

Using a variant of DIQ, we have the following criterion for primary components.

Theorem 2 ([3], Theorem 26)**.** *Let I be an ideal and P a prime divisor of I. For a P-primary ideal Q, if $Q \not\supset (I : P^\infty)$, then the following conditions are equivalent.*

(A) Q is a P-primary component for some primary decomposition of I.

(B) $(I : (I : J)^\infty) = J$ for $J = (I : P^\infty) \cap Q$.

For a given prime divisor, we can check if it is isolated or embedded by the following criterion.

Proposition 3 ([3], Corollary 34)**.** *Let I be an ideal and P a prime divisor of I. Then,*

(i) *P is isolated if $(I : (I : P^\infty)^\infty) \neq K[X]$,*

(ii) *P is embedded if $(I : (I : P^\infty)^\infty) = K[X]$.*

Also, we can compute the *equidimensional hull* $\mathrm{hull}(I)$ of I, the intersection of all primary components of I whose dimension is that of I, by DIQ and a regular sequence as follows.

Proposition 4 ([5], Proposition 3.41)**.** *Let I be an ideal in $K[x_1, \ldots, x_n]$ and $u \subset I$ a regular sequence of length c, where c is the codimension of I i.e. $c = n - \dim(I)$. Then* $\mathrm{hull}(I) = (\langle u \rangle : (\langle u \rangle : I))$.

By combining equidimensional hull and DIQ, we can compute the isolated primary component directly from a given isolated prime divisor as follows.

Theorem 5 ([3], Theorem 36)**.** *Let I be an ideal and P an isolated prime divisor of I. Then*

$$\mathrm{hull}((I : (I : P^\infty)^\infty))$$

is the isolated P-primary component of I.

It is possible to compute embedded primary components from a given embedded prime divisors by the following proposition.

Proposition 6 ([1], Section 4)**.** *Let P be a prime divisor of I. For a sufficiently large integer m,* $\mathrm{hull}(I + P^m)$ *is a P-primary component of I.*

In the above proposition, we can check if m is large enough or not (i.e. $\mathrm{hull}(I + P^m)$ is a primary component or not) by using Theorem 2.

In the talk, we also see other applications of DIQ and its variants. Most of the propositions in the talk are introduced in references [2], [3] and [4].

Keywords
Gröbner basis, Ideal Operation, Localization, Primary Decomposition

References

[1] D. Eisenbud, C. Huneke, W. Vasconcelos, *Direct methods for primary decomposition*. Inventi. Math., **volume**(110), 207–235 (1992).

[2] Y. Ishihara, Modular techniques for effective localization and double ideal quotient. In *Proceedings of ISSAC '20*, 265–272, (2020).

[3] Y. Ishihara, K. Yokoyama, Effective localization using double ideal quotient and its implementation. In *Computer Algebra in Scientific Computing, CASC 2018*, 272–287, (2018).

[4] Y. Ishihara, K. Yokoyama, Computation of a primary component of an ideal from its associated prime by effective localization. *Communications of Japan Society for Symbolic and Algebraic Computation* **volume**(4), 1–31, (2020).

[5] W. Vasconcelos, *Computational Methods in Commutative Algebra and Algebraic Geometry*. Algorithms and Computation in Mathematics **volume**(2), (2004).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algorithms for Polynomial System Solving and Their Applications”*

Noetherian representations for zero-dimensional ideals

Katsusuke Nabeshima[1]**, *Shinichi Tajima***[2] [nabeshima@rs.tus.ac.jp]

[1] Department of Applied Mathematics, Tokyo University of Science, Tokyo, Japan
[2] Graduate School of Science and Technology, Niigata University, Niigata, Japan

We introduce an effective algorithm for computing Noetherian differential operators of zero-dimensional primary ideals and present a new representation of a zero-dimensional ideal. We show that zero-dimensional ideals can be represented by the Noetherian (differential) operators and prime ideals. Moreover, we present new ideal computations as an application.

In 1938 W. Gröbner introduced differential operators to characterize membership in a polynomial ideal [7]. He derived such characterizations for prime or primary ideals and formulated the same problem [7] for any primary ideals.

Let x be an abbreviation of n variables $x_1, \ldots, x_n$, K a field with $\mathrm{char}(K) = 0$, $\partial_{x_i} := \frac{\partial}{\partial x_i}$ $(1 \leq i \leq n)$ and $D_X := K[x][\partial_{x_1}, \ldots, \partial_{x_n}]$ a ring of partial differential operators with coefficients in $K[x]$. If $I \subset K[x]$ is primary and $\sqrt{I} = P$ (the radical of I), then we say that I is P-primary.

L. Ehrenpreis and V. Palamodov gave the following theorem.

Theorem 1. *Let $Q \subset K[x]$ be a $\mathfrak{p}$-primary ideal. There exist partial differential operators $P_1, \ldots, P_\ell$ in D_X with the following property. A polynomial $h \in K[x]$ lies in the ideal Q if and only if $P_1(h), \ldots, P_\ell(h) \in \mathfrak{p}$.*

The partial differential operators $P_1, \ldots, P_\ell$ are called **Noetherian operators** for the primary ideal Q. These partial differential operators represent the difference of Q and the associated prime $\mathfrak{p}$, namely, the operators and the prime $\mathfrak{p}$ completly determine the structure of the primary ideal Q. Therefore, it is important to compute the operators for analyzing the primary ideal.

Recently, in the articles [2,3,4], Noetherian operators have been studied, and an algorithm for computing Noetherian operators have been given. Main tools of the articles are “Hilbert scheme” and “Macaulay’s dual space”.

In this talk, we only consider zero-dimensional ideals and give an algorithm for computing Noetherian operators of zero-dimensional primary ideals. The resulting algorithm is much faster than the algorithm given in [2,3,4], because the resulting algorithm mainly consists of linear algebra computations.

In order to construct the algorithm for computing Noetherian operators, we need the following propositions.

Proposition 1. *Let Q be a zero-dimensional primary ideal in $K[x]$ and $\sqrt{Q} = \mathfrak{p}$. Then, the set of Noetherian operators of Q in D_X is a finite dimensional vector space over the filed $K[x]/\mathfrak{p}$.*

Proposition 2. *Let I be a zero-dimensional ideal generated by $g_1, \ldots, g_m$ in $K[x]$ and Q be a primary component of I with $\sqrt{Q} = \mathfrak{p}$. Let NB_Q be a basis of Noetherian operators of Q in D_X. Then, an arbitrary $P \in \mathrm{NB}_Q$ satisfies the following*
(i) $P(g_i) \in \mathfrak{p}$, $i = 1, \ldots, m$.
(ii) The commutator $[P, x_i] := Px_i - x_iP \in \mathrm{Span}_{K[x]/\mathfrak{p}}(\mathrm{NB}_Q)$.

The outline of our algorithm for computing Noetherian operators is the following.

Outline of the algorithm

Input: $I \subset K[x]$: a zero-dimensional ideal.
Output: $\mathrm{Noether}(I) = \{(\mathfrak{p}_1, \mathrm{NB}_1), \ldots, (\mathfrak{p}_\ell, \mathrm{NB}_\ell)\}$: $\mathfrak{p}_i$ is a associate prime of a primary component Q_i of I. NB_i is a basis of Noetherian operators of Q_i in D_X.

Step 1: Compute a prime decomposition of $\sqrt{I}$.
(Note that there exists an algorithm for computing a prime decomposition of $\sqrt{I}$. The algorithm is much faster than an algorithm for computing a primary decomposition of I. See [1].)
Step 2: (main part) For each prime ideal, compute Noetherian operators of the corresponding primary ideal. Repeat the following.
2-1: Take a candidate ∂^α of head terms.
2-2: Set $f = \partial^\alpha + \sum_{\partial^\alpha \succ \partial^\beta} h_\beta \partial^\beta$ where h_β is indeterminate.
2-3: Check Proposition 2 and decide h_β in $K[x]/\mathfrak{p}$.

Note that the input of the algorithm allows any zero-dimensional ideals.

The algorithm above has been implemented in the computed algebra system Risa/Asir.

We give an example.

Let $f = (x^2 + y^2)^2 + 3x^2y - y^3$, $g = x^2 + y^2 - 1$, and $I = \langle f, g\rangle \subset \mathbb{Q}[x, y]$. First, we compute a prime decomposition of $\sqrt{I}$, i.e.

$$\sqrt{I} = \langle x, y - 1\rangle \cap \langle 4x^3 - 3, 2y + 1\rangle.$$

Let $\mathfrak{p}_1 = \langle x, y - 1\rangle$ and $\mathfrak{p}_2 = \langle 4x^3 - 3, 2y + 1\rangle$. As I is a zero-dimensional ideal, I can be represented by

$$I = Q_1 \cap Q_2$$

where Q_1 is $\mathfrak{p}_1$-primary and Q_2 is $\mathfrak{p}_2$-primary. Our implementation outputs the following

$$\mathrm{Noether}(I) = \{(\mathfrak{p}_1, \{1, \partial_x\}),\ (\mathfrak{p}_2, \{1, \partial_x + 2x\partial_y\})\}$$

as Noetherian representation of the ideal I. The output $\{(\mathfrak{p}_1, \{1, \partial_x\}),\ (\mathfrak{p}_2, \{1, \partial_x + 2x\partial_y\})\}$ can be regared as a primary decomposition of I. Furthermore, we can regard $I = \langle f, g\rangle$ in the same light as $\{(\mathfrak{p}_1, \{1, \partial_x\}),\ (\mathfrak{p}_2, \{1, \partial_x + 2x\partial_y\})\}$.

In general, we call $\mathrm{Noether}(I) = \{(\mathfrak{p}_1, \mathrm{NB}_1), \ldots, (\mathfrak{p}_\ell, \mathrm{NB}_\ell)\}$ Noetherian representation of I.

As an application, we give an example of a sum of ideals. Let Q_1 and Q_2 be $\mathfrak{p}$-primary ideal in $\mathbb{Q}[x, y]$ where $\mathfrak{p} = \langle 4x^2 - 3, 2y + 1\rangle$. Assume that the Noetherian representations of Q_1 and Q_2 are given as

$$\mathrm{Noether}(Q_1) = \{(\mathfrak{p}, \{1, \partial_x, \partial_x^2 - 64x\partial_y\})\},\ \mathrm{Noether}(Q_2) = \{(\mathfrak{p}, \{1, \partial_x, \partial_y, \partial_x\partial_y\})\}.$$

Let's consider $Q_1 + Q_2$, the sum of the ideals. By computing the intersection of the sets of Noetherian operators, we can obtain $\mathrm{Noether}(Q_1 + Q_2)$, actually, since

$$\mathrm{Span}_{\mathbb{Q}[x,y]/\mathfrak{p}}(1, \partial_x, \partial_x^2 - 64x\partial_y) \cap \mathrm{Span}_{\mathbb{Q}[x,y]/\mathfrak{p}}\left(1, \partial_x, \partial_y, \partial_x\partial_y\right) = \mathrm{Span}_{\mathbb{Q}[x,y]/\mathfrak{p}}\left(1, \partial_y\right),$$

we have,

$$\mathrm{Noether}(Q_1 + Q_2) = \{(\mathfrak{p}, \{1, \partial_y\})\}.$$

Base on the concept of Noetherian representations, we can construct a new framework for handing zero-dimensional ideals.

Keywords

Noetherian operators, primary ideals, zero-dimensional ideals

References

[1] T. Aoyama, M. Noro, Modular Algorithms for Computing Minimal Associated Primes and Radicals of Polynomial Ideals, *Proc. ISSAC2018*, 31–38 (2018).

[2] Y. Cid-Ruiz. Noetherian operators, primary submodules and symbolic powers. *Collect. Math.*, **72**, 175–202 (2021).

[3] Y. Cid-Ruiz, R. Homs, and B. Sturmfels. Primary ideals and their differential equations. *Foundations of Computational Mathematics*, (2021). `https://doi.org/10.1007/s10208-020-09485-6`

[4] J. Chen, Y. Cid-Ruiz, M. Härkönen, R. Krone, A. Leykin, Noetherian operators in MACAULAY2, *arXiv:2101.01002*, 2021

[5] L. Ehrenpreis, *Fourier Analysis in Several Complex Variables*. Wily-Interscience Publishers, 1970.

[6] W.Gröbner, *Algebraische Geometrie II*. Hochschultaschenbücger, 1970.

[7] W. Gröbner. Ub̈er eine neue idealtheoretische Grundlegung der von linearen Differentiallgleichungen mit konstanten Koeffizienten. *Monatshefte fur̈ Mathematik und Physik*, **47**, 247–284 (1938).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algorithms for Polynomial System Solving and their Applications”*

An Attempt to Enhance Buchberger’s Algorithm by Using PRSs and GCDs (a Brief Survey)

Tateaki Sasaki[1]***, Masaru Sanuki***[2]***, Daiju Inaba***[3]***, Fujio Kako***[4] [sasaki@math.tsukuba.ac.jp]

[1] Professor emeritus, University of Tsukuba, Tsukuba-shi, Ibaraki 305-8571, Japan
[2] Faculty of Medicine, University of Tsukuba, Tsukuba-shi, Ibaraki 305-8571, Japan
[3] The Mathematics Certification Institute of Japan, Ueno 5-1-1, Tokyo 110-0005, Japan
[4] Nara-Women’s University (previous affiliation), Nara-shi, Nara 630-8506, Japan

By GB we denote the reduced Gröbner basis of polynomial ideal w.r.t. the lexicographic term order. Let the GB of given three-or-more polynomial system $\mathcal{F}$ be $\mathrm{GB}(\mathcal{F}) = \{\widehat{G}_1, \widehat{G}_2, \cdots\}$, where $\widehat{G}_1 \prec \widehat{G}_2 \prec \cdots$. This talk surveys our recent works for computing small multiples or leading-monomial multiples (multiplier is 1 sometimes) of important elements of $\mathrm{GB}(\mathcal{F})$, by the PRSs and GCDs. Let the multiples be $\widetilde{G}_1 \prec \widetilde{G}_2 \prec \cdots$. Our plan is to compute $\mathrm{GB}(\mathcal{F})$ by applying Buchberger’s algorithm to $\mathcal{F} \cup \{\widetilde{G}_1, \widetilde{G}_2, \cdots\}$. Our method is unique in that the multiples are computed as $\widetilde{G}_1 \Rightarrow \widetilde{G}_2 \Rightarrow \cdots$. We note that the coefficient sizes of actual elements of GB are such that $\mathrm{csize}(\widehat{G}_1)$ is almost the smallest among $\mathrm{csize}(\widehat{G}_1), \mathrm{csize}(\widehat{G}_2), \cdots$. This fact suggests us that our approach is reasonable.

Two new theorems are proved, one is for computing the lowest-order element of ideal generated by relatively prime $G, H \in \mathbb{Q}[x, u_1, u_2, \ldots]$, and another is for computing small multiples of elements of $\mathrm{GB}(\mathcal{F})$ efficiently. Two propositions are given for removing still remaining extraneous factors effectively. Four new concepts are introduced, “healthy system”, “rectangular PRSs”, “elimination of LC (leading coefficient) set”, and “LCtoW (LC to Whole) polynomial”. We explain these by using many examples.

Keywords
lexicographic Gröbner basis, polynomial remainder sequence, coefficients of generators

References

[1] T. SASAKI; D. INABA, Simple relation between the lowest-order element of ideal $\langle G, H \rangle$ and the last element of the polynomial remainder sequence. In *Proceedings of SYNASC 2017*, Tudor Jebelean et al. (eds.), 55–62 (2018).

[2] T. SASAKI; D. INABA, Computing the lowest-order element of the elimination ideal of multivariate polynomial system by using remainder sequences. In *Poceedings of SYNASC 2018*, Erika Abraham et al. (eds.), 37–44 (2019).

[3] T. SASAKI, An attempt to emhance Buchberger’s algorithms by using remainder sequences and GCD operation. In *Proccedings of SYNASC 2019*, 27–34 (2020).

[4] T. SASAKI; M. SANUKI; D. INABA; F. KAKO, An attempt to enhance Buchberger’s algorithm by using remainder sequences and GCDs (II). *RIMS Kôkyûroku (Research Reports of Research-Inst.-for-Mathematical-Sciences, Kyoto Univ.) 2185*, 71–80 (2021).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algorithms for Polynomial System Solving and their Applications”*

Proposal of Multivariate Polynomial Arithmetic in a Specified Width of High- or Low-Exponents

Tateaki Sasaki[1]***, Masaru Sanuki***[2]***, Daiju Inaba***[3] [sasaki@math.tsukuba.ac.jp]

[1] Professor emeritus, University of Tsukuba, Tsukuba-shi, Ibaraki 305-8571, Japan
[2] Fuculty of Medicine, University of Tsukuba, Tsukuba-shi, Ibaraki 305-8571, Japan
[3] The Mathematics Certification Institute of Japan, Ueno 5-1-1, Tokyo 110-0005, Japan

The truncated power-series is very useful in computer algebra, however we must control the cutoff degree very carefully when we use the power-series in actual algorithms. In this paper, we propose a much more useful multivariate polynomial arithmetic on the recursive representation of the polynomial. The arithmetic reserves only the terms of high- or low-exponents in a user-specified width w.r.t. a specified variable (other terms are discarded automatically). Of course, the exponents are determined by the conventional arithmetic hence changed as the computation proceeds, while the width (measured from either the highest or the lowest exponent) is fixed.

We obtained this idea in our recent project of enhancing Buchberger's algorithm for the lexicographic Gröbner bases of multivariate polynomial ideals, by using PRSs (Polynomial Remainder Sequences) and GCDs. In our project, PRSs and their “coefficients of generators” (= coefficients of Bezout's identity) are critically important but the computation of them is very heavy. However, what we need are only low-exponents parts in a narrow width, say 1/10 of the exponent range of the full expression. We investigate this idea from practical point of view, and give detailed procedures for realizing this idea definitely. We show several examples of using new arithmetic.

Keywords
polynomial remainder sequence, extended Euclidean algorithm, coefficients of generators

References

[1] T. Sasaki, A theory and an algorithm for computing sparse multivariate polynomial remainder sequence. In: Computer Algebra in Scientific Computing (Proceedings of CASC 2018), Springer LNCS **11077**, 345-360 (2018).

[2] T. Sasaki, An attempt to emhance Buchberger's algorithms by using remainder sequences and GCD operation. In *Proccedings of SYNASC 2019*, 27–34 (2020).

[3] T. Sasaki; M. Sanuki; D. Inaba; F. Kako, An attempt to enhance Buchberger's algorithm by using remainder sequences and GCDs (II). *RIMS Kôkyûroku (Research Reports of Research-Inst.-for-Mathematical-Sciences, Kyoto Univ.) 2185*, 71-80 (2021).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algorithms for Polynomial System Solving and Their Applications”*

Computing holonomic D-modules associated to a family of non-isolated hypersurface singularities via comprehensive Gröbner systems of PBW algebra

Shinichi Tajima[1]***, Katsuyoshi Ohara***[2]***, Katsusuke Nabeshima***[3] [tajima@math.tsukuba.ac.jp]

[1] Graduate School of Science and Technology, Niigata University, Niigata, Japan
[2] Faculty of Mathematics and Physics, Kanazawa University, Kanazawa, Japan,
[3] Department of Applied Mathematics, Tokyo University of Science, Tokyo, Japan

We consider holonomic D-modules and microlocal b-functions associated to a family of non-isolated hypersurface singularities in the context of symbolic computation. We present an algorithm for computing them and describe a method for analyzing the structure of holonomic D-modules to compute microlocal b-functions. The key of the proposed method is the concept of local cohomology [1].

Let $f(x) \in K[x] = K[x_1, x_2, \cdots, x_n]$ be a polynomial of n variables with coefficients in a field K of characteristic zero. Let D denote the Weyl algebra:

$$D = K[x, \tfrac{\partial}{\partial x}] = K[x_1, x_2, \cdots, x_n, \tfrac{\partial}{\partial x_1}, \tfrac{\partial}{\partial x_2}, \cdots, \tfrac{\partial}{\partial x_n}].$$

Let $D[s] = D \otimes_K K[s]$, where s is an indeterminate. A b-function, or Bernstein-Sato polynomial, is defined to be a monic generator of the ideal consisting of the polynomials $b(s)$ that satisfy $b(s)f^s = P(s, x, \frac{\partial}{\partial x})f^{s+1}$ for some partial differential operator $P \in D[s]$. For the case where the hypersurface $S = \{x \in \mathbb{C}^n \mid f(x) = 0\}$ defined by f has non-isolated singularity, the (microlocal) b-functions and relevant holonomic D-modules are crucial in the study of singularity of the hypersurface S.

In this talk, we consider the case where the defining polynomial contains deformation parameters. More precisely, we consider the case

$$f_u(x) \in (K[u])[x] = K[u_1, u_2, \cdots, u_\ell, x_1, x_2, \cdots, x_n],$$

where $u = (u_1, u_n, \cdots, u_\ell)$ is regarded as a set of parameters. Based on our previous work [5] on comprehensive Gröbner basis in Poincaré-Birkhoff-Witt algebra, we extend the method given in [6] to parametric cases and present a new approach to studying deformation of non-isolated singularities.

In order to illustrate our approach, we will study and compute in particular the following examples.

Example 1 (D. B. Massey, 1990 [3])

$$f(x,y,z,w) = w^2 - yz^2 - xz^3 - z^4.$$

Example 2 (D. B. Massey, 1995 [4])

$$f(x,y,w_1,w_2,w_3) = y^2 - x^3 - (w_1^2 + w_2^2 + w_3^2)x^2.$$

Example 3 (D. B. Massey, 1995 [4])

$$f_u(x,y,z) = x^2 - y^3 - uzy^2$$

where u is a parameter.

Example 4 (J. Fernandez de Bobadilla, 2005 [1])

$$f_u(x_1,x_2,x_3,y_1,y_2) = x_3y_1^2 + 2x_2y_1y_2 + (ux_1 - x_3)y_2^2.$$

where u is a parameter.

Keywords
holonomic D-modules, non-isolated hypersurface singularities, comprehensive Gröbner systems, PBW algebra

References

[1] J. FERNANDEZ DE BOBADILLA, Answer to some equisingularity questions. *Invent. math.* **161**, 657–675 (2005).
[2] M. KASHIWARA, On the holonomic systems of linear differential equations. II. *Invent. math.* **49**, 121–142 (1978).
[3] D. B. MASSEY,The Lê varieties, I. *Invent. math.* **99**, 357–376 (1990).
[4] D. B. MASSEY, *Lê Cycles and Hypersurface Singularities.* Lecture Notes in Math. **1615** (1995).
[5] K. NABESHIMA, K. OHARA AND S. TAJIMA, Comprehensive Gröbner systems in PBW algebra, Bernstein-Sato ideals and holonomic D-modules. *J. Symbolic Compt.* **89**, 146–170 (2018).
[6] S. TAJIMA AND Y. UMETA, Holonomic D-module4s associated with a simple line singularity and the vertical monodromy. *Funkcialaj Ekvacioj* **64**, 17–48 (2021).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Algorithms for Polynomial System Solving and Their Applications*

Some tips on the implementation of CGS in SageMath

Miwa Taniwaki[1]***, Yosuke Sato***[2] [1420516@ed.tus.ac.jp]

[1] Graduate school of Science, Tokyo University of Science, Tokyo, Japan
[2] Department of Applied Mathematics, Tokyo University of Science, Tokyo, Japan

A comprehensive Gröbner system (CGS) is a powerful tool for handling parametric polynomial systems. Its first practical computation algorithm was introduced in [6]. With improvements of the subsequent works such as [3,4,5], we now have several its application programs such as the one introduced in [2].

It seems that a basic framework of its practical computation algorithm was established by the work of [5] at least from a theoretical point of view, however, there still remain many important issues concerning its efficient implementation. We have developed several techniques which improve the existing implementations of CGS. Our methods require several ideal manipulations such as the computations of radical ideals or saturation ideals. Even though those computations are rather heavy in general, we have observed our techniques are quite effective through our implementation in SageMath [1].

In the talk, we introduce our techniques through an interesting example of geometry theorem proving(discovery) which is one of the most typical applications of CGS.

Keywords
Comprehensive Gröbner System, SageMath

References

[1] *SageMath*, A free open-source mathematics software system licensed under the GPL. https://www.sagemath.org/
[2] R. FUKASAKU; H. IWANE; Y. SATO, *Real Quantifier Elimination by Computation of Comprehensive Gröbner Systems.* Proceedings of International Symposium on Symbolic and Algebraic Computation, pp. 173–180, ACM, 2015.
[3] D. KAPUR; Y. SUN; D. WANG, *A New Algorithm for Computing Comprehensive Gröbner Systems.* Proceedings of International Symposium on Symbolic and Algebraic Computation, pp. 29–36, ACM, 2010.
[4] Y. KURATA, *Improving Suzuki-Sato's CGS Algorithm by Using Stability of Gröbner Bases and Basic Manipulations for Efficient Implementation.*, Communications of the Japan Society for Symbolic and Algebraic Computation, Vol. 1, pp. 39–66, JSSAC, 2011.
[5] K. NABESHIMA, *Stability Conditions of Monomial Bases and Comprehensive Gröbner*

systems., Lecture Notes in Computer Science, Vol. 7442, pp. 248–259, Springer, 2012.

[6] A. SUZUKI; Y. SATO, *A Simple Algorithm to Compute Comprehensive Gröbner Bases Using Gröbner Bases.* Proceedings of International Symposium on Symbolic and Algebraic Computation, pp. 326–331, ACM, 2006.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algorithms for Polynomial System Solving and Their Applications”*

Polynomial Coefficients of Elimination Results from a system of Classical Mechanics

Jonathan Tot[1], ***Robert H. Lewis***[2] [jonathan.tot@dal.ca]

[1] Department of Mathematics and Statistics, Dalhousie University, Halifax, NS
[2] Mathematics Department, Fordham University, Bronx, NY

In work that is being prepared for publication, we study the static solutions of a rotating double pendulum: a double pendulum modeled as constructed from physical pendula, or three-dimensional rigid bodies, and made to rotate uniformly about the vertical axis through the fixed inner pivot. Resultants can be computed to produce bifurcation diagrams: plots of equilibrium positions against a control parameter. Bifurcation can also be described by a system of polynomial equations. Variables corresponding to an equilibrium configuration can be eliminated from the system, producing a polynomial condition on the parameter space; the model exhibits bifurcation for parameter values which are roots of the resultant. This and other related resultants have been computed using `DixonEDF`[2], an algorithm which extracts a factorization of the Dixon resultant, and which is implemented in the CAS *Fermat*. In this presentation, we will also present several observations of novel patterns observed in the coefficient arrays of the large polynomials produces by these computations.

Keywords
Polynomial System Solving, Elimination, Resultants, Discriminant, Polynomial Coefficients

References

[1] S. MAITI ET AL., Nonlinear dynamics of a rotating double pendulum. *Physics Letters A* **380**, 408–412 (2016).
[2] R.H. LEWIS, Dixon-EDF: The Premier Method for Solution of Parametric Polynomial Systems. In *Applications of Computer Algebra. ACA 2015. Springer Proceedings in Mathematics & Statistics, vol 198*, I. Kotsireas, E. Martínez-Moro (eds.), 237-256. Springer, Cham, 2017.

S15. Symbolic and Exact Linear Algebra over Rings and Fields

Organized by

Mark Giesbrecht, Armin Jamshidpey and Eric Schost

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Symbolic and Exact Linear Algebra over Rings and Fields*

Applications of the Smith massager of a nonsingular integer matrix

Stavros Birmpilis[1]***, George Labahn***[1]***, Arne Storjohann***[1] [sbirmpil@uwaterloo.ca]

[1] Cheriton School of Computer Science, University of Waterloo, Canada

Given a nonsingular integer matrix $A \in \mathbb{Z}^{n \times n}$ with Smith normal form $S = \mathrm{diag}(s_1, \ldots, s_n)$, we define a matrix $M \in \mathbb{Z}^{n \times n}$ to be a Smith massager for A. Matrix M satisfies (i) that $AM \equiv 0 \ \mathbf{c}\mathrm{mod}\ S$, namely, the matrix AMS^{-1} is integral, and (ii) that there exists a matrix $W \in \mathbb{Z}^{n \times n}$ such that $WM \equiv I_n \ \mathbf{c}\mathrm{mod}\ S$, namely, the Smith massager is "unimodular" up to equivalence column modulo S. We obtain the Smith massager from the algorithm in [1] that computes the Smith form of A. We show that it can be used to solve other problems in integer linear algebra like computing the Smith multiplier matrices for A or the Hermite form of A.

Keywords
Smith form, Hermite form

References

[1] S. BIRMPILIS; G. LABAHN; A. STORJOHANN, A Las Vegas algorithm for computing the Smith form of a nonsingular integer matrix. In *Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation*, 38–45. ACM, New York, NY, 2020.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Symbolic and Exact Linear Algebra over Rings and Fields*

Exact linear algebra over the complex numbers

Fredrik Johansson[1] [fredrik.johansson@gmail.com]

[1] Inria and Institut. Math. Bordeaux, Talence, France

Linear algebra over the complex numbers presents three difficulties: expression growth for exact representations, precision loss for inexact representations, and the problem of testing for zero. These difficulties are especially notable over transcendental number fields, but there are practical efficiency concerns already in the case of algebraic number fields of high degree. I will review algorithms for fundamental matrix operations (multiplication, solving, determinant, characteristic polynomial, eigenvalues) in an exact setting and discuss implementation results in the Calcium library [1, 2].

Keywords
Exact linear algebra, number fields

References

[1] F. Johansson, Calcium: computing in exact real and complex fields. In *ISSAC '21*, Jul 2021, Virtual Event, Russia. 10.1145/3452143.3465513. https://hal.inria.fr/hal-02986375v2
[2] F. Johansson, On a fast and nearly division-free algorithm for the characteristic polynomial, 2020, https://hal.inria.fr/hal-03016034

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Symbolic and Exact Linear Algebra over Rings and Fields*

Deterministic computation of the characteristic polynomial in the time of matrix multiplication

Vincent Neiger[1]***, Clément Pernet***[2] [vincent.neiger@unilim.fr]

[1] Univ. Limoges, CNRS, XLIM, UMR 7252, F-87000 Limoges, France
[2] Université Grenoble Alpes, Laboratoire Jean Kuntzmann, CNRS, UMR 5224, 700 avenue centrale, IMAG - CS 40700, 38058 Grenoble cedex 9, France

The last five decades witnessed a constant effort towards computational reductions of linear algebra problems to matrix multiplication. It has been showed that most classical problems are not harder than multiplying two square matrices, such as matrix inversion, LU decomposition, nullspace basis computation, linear system solving, rank and determinant computations, etc. [1] [2, Chap. 16] [3]. In this context, one major challenge stands out: designing a similar reduction to matrix multiplication for the computation of characteristic polynomials and related objects such as minimal polynomials and Frobenius forms. For the characteristic polynomial, significant progress was achieved by Keller-Gehrig [4], and more recently by Pernet and Storjohann [6] who solved the problem if one allows randomization.

In this talk, we report on a recent result [5] which closes the problem by providing a deterministic algorithm with the same asymptotic complexity as matrix multiplication. Previously, this was only achieved by resorting to genericity assumptions or randomization techniques, while the best known complexity bound with a general deterministic algorithm was obtained by Keller-Gehrig in 1985 and involves logarithmic factors. Our algorithm computes more generally the determinant of a univariate polynomial matrix in reduced form, and relies on new subroutines for transforming shifted reduced matrices into shifted weak Popov matrices, and shifted weak Popov matrices into shifted Popov matrices.

The characteristic polynomial of a square matrix over a field $\mathbb{K}$, say $M \in \mathbb{K}^{m\times m}$, is defined as $xI_m - M)$. Specific algorithms exist for sparse or structured matrices; here we consider the classical, dense case. Here, the complexity of an algorithm is measured as an upper bound on its arithmetic cost, that is, the number of basic field operations it uses to compute the output.

Theorem. Using a subroutine which multiplies two matrices in $\mathbb{K}^{m\times m}$ in $O(m^\omega)$ field operations for some $\omega > 2$, the characteristic polynomial of a matrix in $\mathbb{K}^{m\times m}$ can be computed deterministically in $O(m^\omega)$ field operations.

Keywords
Characteristic polynomial, Polynomial matrices, Determinant, Fast linear algebra

References

[1] Bunch, J.R. and Hopcroft, J.E., 1974. Triangular factorization and inversion by fast matrix multiplication. Mathematics of Computation 28, 231–236.

[2] Bürgisser, P., Clausen, and M., Shokrollahi, A., 1997. Algebraic Complexity Theory. 1st ed., Springer-Verlag Berlin Heidelberg.

[3] Ibarra, O.H., Moran, S., and Hui, R., 1982. A generalization of the fast LUP matrix decomposition algorithm and applications. Journal of Algorithms 3, 45–56.

[4] Keller-Gehrig, W., 1985. Fast algorithms for the characteristic polynomial. Theoretical Computer Science 36, 309–317.

[5] Neiger, V. and Pernet, P. Deterministic computation of the characteristic polynomial in the time of matrix multiplication, Journal of Complexity, 2021.

[6] Pernet, C., Storjohann, A., 2007. Faster Algorithms for the Characteristic Polynomial, in: ISSAC'07, ACM. pp.307–314.

Null ideals of square matrices over residue class rings of PIDs

Roswitha Rissner [1], ***Clemens Heuberger***[1] [roswitha.rissner@aau.at]

[1] Department of Mathematics, University of Klagenfurt, Austria

Given a square matrix $\tilde{B}$ over a (commutative) ring S, the null ideal $\mathsf{N}_0(\tilde{B})$ is ideal consisting of all polynomials $f \in S[X]$ for which $f(\tilde{B}) = 0$. In the case that $S = R/J$ is the residue class ring of a ring R modulo an ideal J, we can equivalently study the so-called J-ideals

$$\mathsf{N}_J(B) = \{f \in R[x] \mid f(B) \in M_n(J)\}$$

where B is a preimage of $\tilde{B}$ under the projection modulo J.

If R is a principal ideal domain it suffices to determine a finite number of polynomials in order to describe all J-ideals of B. In this talk we discuss an algorithmic approach to compute these polynomials.

Keywords
null ideals, J-ideals

References

[1] C. HEUBERGER; R. RISSNER, Computing J-ideals of a matrix over a principal ideal domain. *Linear Algebra Appl.* **volume** 527, 12–31 (2017).
[2] R. RISSNER, Null ideals of matrices over residue class rings of principal ideal domains. *Linear Algebra Appl.* **volume** 494, 44–69 (2016).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Symbolic and Exact Linear Algebra over Rings and Fields*

Efficient verification for polynomial matrix computations

***Clément Pernet*[1], *David Lucas*[1], *Vincent Neiger*[2], *Daniel S. Roche*[3], *Johan Rosenkilde*[4]**
[roche@usna.edu]

[1] Laboratoire Jean Kuntzmann, Université Grenoble Alpes, France
[2] Université de Limoges, France
[3] Computer Science Department, United States Naval Academy, Annapolis, Maryland, USA
[4] GitHub, Denmark

We develop and analyze new protocols to verify the correctness of various computations on matrices over $\mathsf{F}[x]$, where F is a field. The properties we verify concern an $\mathsf{F}[x]$-module and therefore cannot simply rely on previously-developed linear algebra certificates which work only for vector spaces. Our protocols are interactive certificates, often randomized, and featuring a constant number of rounds of communication between the prover and verifier. We seek to minimize the communication cost so that the amount of data sent during the protocol is significantly smaller than the size of the result being verified, which can be useful when combining protocols or in some multi-party settings. The main tools we use are reductions to existing linear algebra certificates and a new protocol to verify that a given vector is in the $\mathsf{F}[x]$-linear span of a given matrix.

Keywords
Polynomial matrices, interactive certificates, verifiable computing

References

[1] C. PERNET; D. LUCAS; V. NEIGER; D. ROCHE, J. ROSENKILDE, *Verification protocols with sub-linear communication for polynomial matrix operations*. J. Symb. Comput. 105: 165-198 (2021).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Symbolic and Exact Linear Algebra over Rings and Fields*

Frobenius Normal Form: what, why, and how to compute

B. David Saunders[1] [saunders@udel.edu]

[1] University of Delaware

The LinBox library was launched in the 1990s to implement and exploit blackbox algorithms in high performance linear algebra. Smith Normal Form has been a focus from the beginning, however a Frobenius Normal Form implementation has only recently emerged. I will discuss the reasons for this difference and make the case that normal forms are the essence of exact linear algebra computation and deserve wider use in practice. Greater use can be made of Frobenius form in particular.

Regarding algorithm design, I will illustrate the value of small block size projections and discuss recent improvements in performance and in probabilistic analysis, particularly relevant when working over small fields. I'll discuss some of the awkward choices faced by the implementer and indicate where theory could help.

Keywords
Frobenius Normal Form, LinBox library, Exact linear algebra

References

[1] HARRISON, G., JOHNSON, J. R., AND SAUNDERS, B. D., Probabilistic analysis of block wiedemann for leading invariant factors. *Journal of Symbolic Computation* (to appear 2021).

[2] VILLARD, G., Computing the frobenius normal form of a sparse matrix. In *Computer Algebra in Scientific Computing*, V. G. Ganzha, E. W. Mayr, and E. V. Vorozhtsov, (eds.), 395–407. Editor(s), Berlin, Heidelberg, 2000.

[3] ZEE, F. G. V., SMITH, T. M., MARKER, B., LOW, T. M., GEIJN, R. A. V. D., IGUAL, F. D., SMELYANSKIY, M., ZHANG, X., KISTLER, M., AUSTEL, V., GUNNELS, J. A., AND KILLOUGH, L., The blis framework: Experiments in portability. *ACM Trans. Math. Softw.* **42** (2), 1–19 (2016).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Symbolic and Exact Linear Algebra over Rings and Fields"*

Fast and Practical Algorithms for Solving Linear Systems over Number Fields

Jayantha Suranimalee[1], ***Claus Fieker***[2] [suranimalee@maths.cmb.ac.lk]

[1] Department of Mathematics, University of Colombo, Sri Lanka.
[2] Fachbereich Mathematik, Universität Kaiserslautern, Germany.

We present a deterministic algorithm for solving a non-square linear system over number fields. As the solution is not unique, we compute a basis for the kernel to normalize the solution. The implementation accompanied with a fast algorithm to compute a kernel basis and the reduced row echelon form of a matrix of any size. A modified version of the Dixon algorithm is used in each cases [1]. Here, we use a simple and fast vector reconstruction method to find the solution from the lifting output. We rigorously assess the complexity as $O^{\sim}(m^3d^2 + m^2nd + m^2d^5)$ operations over $\mathbb{Z}$, where as the Gaussian method takes $O^{\sim}(m^3n^2d^2)$ operations to solve a linear $m \times n$ system $Ax = b$ over number field of degree d.

Keywords
non-square linear system, kernel, preconditioning techniques, vector reconstruction

References

[1] J. D. DIXON, Exact solution of linear equations using P-adic expansions. *Numerische Mathematik* **40**(1), 137–141 (1882).

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Symbolic and Exact Linear Algebra over Rings and Fields*

Coppersmith's block Wiedemann method for polynomial problems

Gilles Villard [gilles.villard@ens-lyon.fr]

CNRS, ENS de Lyon, Inria, UCBL, Univ. Lyon, LIP laboratory, Lyon, France

Coppersmith has introduced a block version of Wiedemann's algorithm [1,11]. The method allows to obtain algorithms with best known complexity bounds for various matrix and polynomial problems. We can mention for example:

- Determinant of a matrix over a ring [5];
- Sparse linear systems and inversion of sparse matrices [4, 2, 8];
- Annihilating polynomials of structured matrices [6];
- Resultant of bivariate polynomials [10];
- Fast modular composition of univariate polynomials [7];
- Manipulation of zero-dimensional ideals [3].

We will review the general approach and discuss new improvement for the resultant problem, using a combination of techniques for structured matrices and high-order lifting [9].

Keywords
Coppersmith's block Wiedemann algorithm, resultant of polynomials, structured matrices

References

[1] D. COPPERSMITH, *Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm*. Mathematics of Computation, 62(205), 1994.

[2] W. EBERLY, M. GIESBRECHT, P. GIORGI, A. STORJOHANN, G. VILLARD, *Faster inversion and other black box matrix computation using efficient block projections*. Proc. ISSAC, Waterloo, Canada, ACM Press, 2007.

[3] S. G. HYUN, V. NEIGER, H. RAHKOOY, É. SCHOST., *Block-Krylov techniques in the context of sparse-FGLM algorithms*. Journal of Symbolic Computation, 98, 2020.

[4] E. KALTOFEN, *Analysis of Coppersmith's block Wiedemann algorithm for the parallel solution of sparse linear systems*. Mathematics of Computation, 64(210), 1995.

[5] E. KALTOFEN, G. VILLARD, *On the complexity of computing determinants*. Computational Complexity, 13:91-130, 2005.

[6] P. KARPMAN, C. PERNET, H. SIGNARGOUT, G. VILLARD., *Computing the characteristic polynomial of generic Toeplitz-like and Hankel-like Matrices*. Proc. ISSAC, Saint Petersburg, Russia, ACM Press, 2021.

[7] V. NEIGER, B. SALVY, É. SCHOST, G. VILLARD, *Fast modular composition*. In preparation.

[8] R. PENG, S. VEMPALA, *Solving sparse linear systems faster than matrix multiplication*. Proc. ACM-SIAM SODA, 2021.

[9] A. STORJOHANN, *High-order lifting and integrality certification*. Journal of Symbolic Computation, 36, 2003.

[10] G. VILLARD, *On computing the resultant of generic bivariate polynomials*. Proc. ISSAC, New York, USA, ACM Press, 2018.

[11] D. WIEDEMANN, *Solving sparse linear equations over finite fields*. IEEE Trans. Information Theory 32(1):54–62, 1986.

ACA2021 Volunteers

Bernhard Garn, MATRIS Research Group, SBA Research, Austria

Ludwig Kampel, MATRIS Research Group, SBA Research, Austria

Manuel Leithner, MATRIS Research Group, SBA Research, Austria

Michael Wagner, MATRIS Research Group, SBA Research, Austria

Klaus Kieseberg, MATRIS Research Group, SBA Research, Austria

Dominik-Philip Schreiber, MATRIS Research Group, SBA Research, Austria

Irene Hiess, MATRIS Research Group, SBA Research, Austria

Enrico Lurlano, MATRIS Research Group, SBA Research, Austria

Nikolas Petri, Strategic Innovation and Communication Team, SBA Research, Austria