ACA 2019 | 25TH CONFERENCE ON APPLICATIONS OF COMPUTER ALGEBRA

Montréal, Canada | July 16-20, 2019 | 16 au 20 juillet 2019

PROGRAMME | PROGRAM

ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
Université du Québec

ÉTS
Le génie pour l'industrie

aca2019.etsmtl.ca

ACA2019 | #ACA2019MTL


etsmtl.ca
LA PASSION ÉTS DANS NOS GÈNES.
MA
8 m/s²
a
Ff
Fg
Fz
FY
d
F = ma
122°
49°
FN
Fi
Fj
GRF = 2004 N
FY
ÉTS
Le génie pour l'industrie

The electronic version of this booklet can be found at:
http://aca2019.etsmtl.ca

The codes used to generate this booklet, including the LaTeX template, are available at
https://github.com/maximelucas/AMCOS_booklet

Contents

Bienvenue | Welcome

Chers amis d'ACA,

Nous avons le grand plaisir de vous accueillir à la 25e édition de la Conference on Applications of Computer Algebra (ACA 2019). Dix ans après la conférence ACA 2009, nous sommes ravis d'accueillir cet événement une fois de plus sur le campus de l'École de technologie supérieure (ÉTS). Cette année, la conférence ACA 2019 réunit plus de 140 participants d'une vingtaine de pays. Nous souhaitons un accueil chaleureux à tous ceux et celles qui sont venus de l'extérieur de Montréal pour cette conférence.

Depuis que notre proposition d'accueillir la conférence a été approuvée en 2016, nous attendons cet événement avec impatience. À notre retour de ACA 2018 à Saint-Jacques-de-Compostelle, nous avons commencé à préparer de manière intensive cette conférence. Après plusieurs mois de travail, nous espérons que ACA 2019 sera à la hauteur de vos attentes et que vous repartirez avec des souvenirs inoubliables.

Nous voudrions remercier toutes les personnes qui ont rendu la tenue de ACA 2019 possible. Merci aux conférenciers invités, aux responsables du programme, au groupe de travail de ACA, aux responsables de sessions et à tous les participants. Un merci tout particulier à Étienne Cormier Blouin et Florence Allegrini pour le soutien logistique ainsi qu'à Fatima Gissele Reynosa et Véronique Cadrin pour leur aide précieuse. Merci aussi à nos généreux collègues qui ont accepté d'être bénévoles.

Nous sommes également profondément reconnaissants à l'administration de l'ÉTS : François Gagnon, directeur général de l'ÉTS, Pierre Dumounchel, ancien directeur général, Michel Huneault, directeur des affaires académiques et Frédérick Henri, directeur du Service des enseignements généraux.

Nous vous souhaitons un merveilleux séjour à Montréal. Bonne conférence !

* * *

Dear ACA friends,

It is our great pleasure to welcome you to the 25th edition of the Conference on Applications of Computer Algebra (ACA 2019). Ten years after ACA 2009, we are delighted to be hosting the conference once more on the campus of École de technologie supérieure (ÉTS). This year, ACA 2019 is bringing together over 140 participants from 20 countries. We wish to extend an especially warm welcome to all those who have travelled from outside of Montréal for this conference.

Since our proposal to host the conference was approved in 2016, we have been looking forward to this event. Upon our return from Santiago de Compostella for ACA 2018, we have been preparing for this conference intensively. After several months of hard work, we hope ACA 2019 will live up to your expectations and bring unforgettable memories.

We would like to thank everyone who made ACA 2019 possible. We thank our invited speakers, the program chairs, the ACA working group, the session chairs and all participants. Special thanks to Étienne Cormier Blouin and Florence Allegrini for logistical support, and to Fatima Gissele Reynosa and Véronique Cadrin for their invaluable help. Thank you also to our supportive colleagues who have agreed to volunteer.

We are also deeply grateful to the ÉTS administration: François Gagnon, Director general of ÉTS, Pierre Dumounchel, former Director general, Michel Huneault, Director of Academic Affairs and Frédérick Henri, Director of the Service des enseignements généraux.

We wish you a wonderful stay in Montréal. Bonne conférence!

Comité organisateur | Organizing committee

Michel Beaudin   Anouk Bergeron-Brlek   Louis-Xavier Proulx   Hanan Smidi

Responsables du programme | Program Chairs

Michel Beaudin   Michael Wester

Mot de la mairesse | Word from the Mayor

À l'occasion de son 25^{e} anniversaire, je suis heureuse d'offrir mes plus chaleureuses félicitations aux organisateurs des conférences ACA et je souhaite la bienvenue à tous les participantes et participants, d'ici et d'ailleurs.

Ville de savoir et d'éducation, Montréal comprend bien la valeur de la science et de la technologie. À titre de collectivité, nous nous devons de soutenir et de reconnaître l'expertise et les innovations qui émergent de ces secteurs d'activités.

La connaissance scientifique, la curiosité, la créativité représentent des atouts pour l'avenir de notre métropole. Pour continuer à se développer, à se démarquer, à performer, Montréal a besoin de promouvoir les échanges scientifiques.

Je tiens à saluer l'École de technologie supérieure, qui accueille cette conférence pour la deuxième fois depuis 2009. L'ÉTS, étant la deuxième plus importante faculté de génie au Canada, est reconnue comme une des institutions les plus dynamiques pour son approche innovante en enseignement.

Mes meilleurs vœux de succès accompagnent les organisateurs et organisatrices de cet événement. Par votre dynamisme et votre engagement envers la science, vous contribuez à nourrir la vitalité et la créativité de Montréal.

Je souhaite que cette 25^{e} conférence soit l'occasion d'enrichissantes discussions.

* * *

On the 25th anniversary of its inception, I am pleased to offer my warmest congratulations to the organizers of the ACA conferences and welcome all participants from here and abroad.

As a city of knowledge and education, Montreal understands the value of science and technology. As a community, we have a responsibility to support and recognize the expertise and innovations that emerge from these sectors of activity.

Scientific knowledge, curiosity and creativity are assets for the future of our metropolis. To continue to develop, stand out and perform, Montréal needs to promote scientific exchanges.

I would like to acknowledge the École de technologie supérieure, which is hosting this conference for the second time since 2009. As the second largest engineering school in Canada, ÉTS is recognized as one of the most dynamic institutions for its innovative approach to teaching.

My best wishes for success go to the organizers of this event. Thanks to your energy and commitment to science, you contribute to nurturing Montreal's vitality and creativity.

I hope that this 25th conference will be an opportunity for enriching discussions.

Valérie Plante
Mairesse de Montréal
Mayor of Montréal
Montréal

General Information

Identification badge and lunch vouchers

You must wear your identification badge at all times. The delegate badge gives you access to the **Welcome Reception**, the keynote lectures and talks, the **coffee breaks** and the **excursion**. You don't need your badge for the banquet since there will be a registration table onsite.

With your badge, you have 3 **lunch vouchers** for Wednesday, Thursday and Friday. You must hand the voucher to the cashier at the cafeteria (Pavillon A) in order to pay for lunch. You can choose among all available options such as the sautéed bowls, the baja bar, the snack bar and the chef's table. Your meal cannot exceed $15. There is no voucher provided for lunch on Saturday, but the attendees are invited to join the organizing committee to a nearby restaurant (see section Closing ceremony).

Registration desk

The delegates can pick up their conference documents and get information at the registration desk located next to the main entrance of Pavillon E (1220 rue Notre-Dame Ouest). Registration is available on Tuesday July 16, 16:00 to 18:00 and Wednesday July 17, 8:30 to 9:00.

Conference rooms

- Atrium (E-2010 and E-2011) : Welcome session, coffee breaks and Poster session
- Salon des diplômés Vidéotron (E-2033) : Keynote lectures and ACA Working Group meeting
- E-4024, E-4025, E-4026, B-0904 and B-0906 : Special session talks

Rooms in Pavillon E have whiteboards with markers and rooms in Pavillon B have blackboards with white chalks. Each conference room has a computer running Windows 10 with Internet access, a projector and HDMI and VGA cables for delegates using their laptops.

The following software is available on all computers: Derive 6.10, Maple 2017, Matlab R2016b, DPGraph, Microsoft Office 2016 (French version), Mozilla Firefox 60, Google Chrome, TI-Nspire CX CAS 4.5, Cinderella 2, Geogebra Classic 5, and Acrobat Reader 2019.

Speakers are encouraged to test their material as soon as possible. Volunteers will be giving technical assistance at the beginning of each talk.

Meeting spaces

Lounge space in the Atrium (E-2010) and the library (ground floor of Pavillon A) can be used by delegates for impromptu meetings and discussions during the conference.

Maplesoft booth

All conference delegates are invited to visit the Maplesoft booth. You will find it in the Atrium (E-2011) next to the coffee break tables.

Internet

Here are two network options for wifi access:

ETS-Invites
Choose the network `ETS-Invites`. Once the connection is established, open a browser. You should automatically be brought to a web portal at `https://wifiets.etsmtl.ca`. You can then complete the identification step on the network:

Nom d'utilisateur (username): `wifi-aca@etsmtl.ca`
Mot de passe (password): `Algebra2019`

Eduroam
If your institution is a member of the eduroam network, you can connect to `eduroam` with your username (your university email address) and password (associated with the username).

Social media

You can follow `@ACA2019` on Twitter and Facebook. Please use the `#ACA2019MTL` hashtag when sharing content and pictures during the conference.

Sports facilities

You have access to the Centre Sportif ÉTS, with its training center, locker rooms, and showers. The Centre Sportif is located on the third floor of Pavillon B. The access is granted upon showing your identification badge to the employee at the counter.

If you choose to use the showers, bring a lock and a towel.

If you want to use the gym, you must bring a towel and wear sportswear (bags and coats must stay in the locker room). You must also fill a short mandatory fitness questionnaire for insurance purposes.

Contact information

If you need more information about ACA 2019, please check our website: `aca2019.etsmtl.ca`. For any inquiries, please send an email to the organizing committee at `aca2019@etsmtl.ca`.

The CARGO Lab is proud to be a gold sponsor of the ACA 2019 conference, the 25th Conference on Applications of Computer Algebra in the ACA series. The ACA conference series returns to the École de technologie supérieure (ÉTS) in Montréal for the second time in a decade, which showcases the incredible energy and enthusiasm of our colleagues there. I am certain that ACA 2019 will be a great success!

Ilias S. Kotsireas, Director, CARGO Lab, co-chair ACA Working Group

---

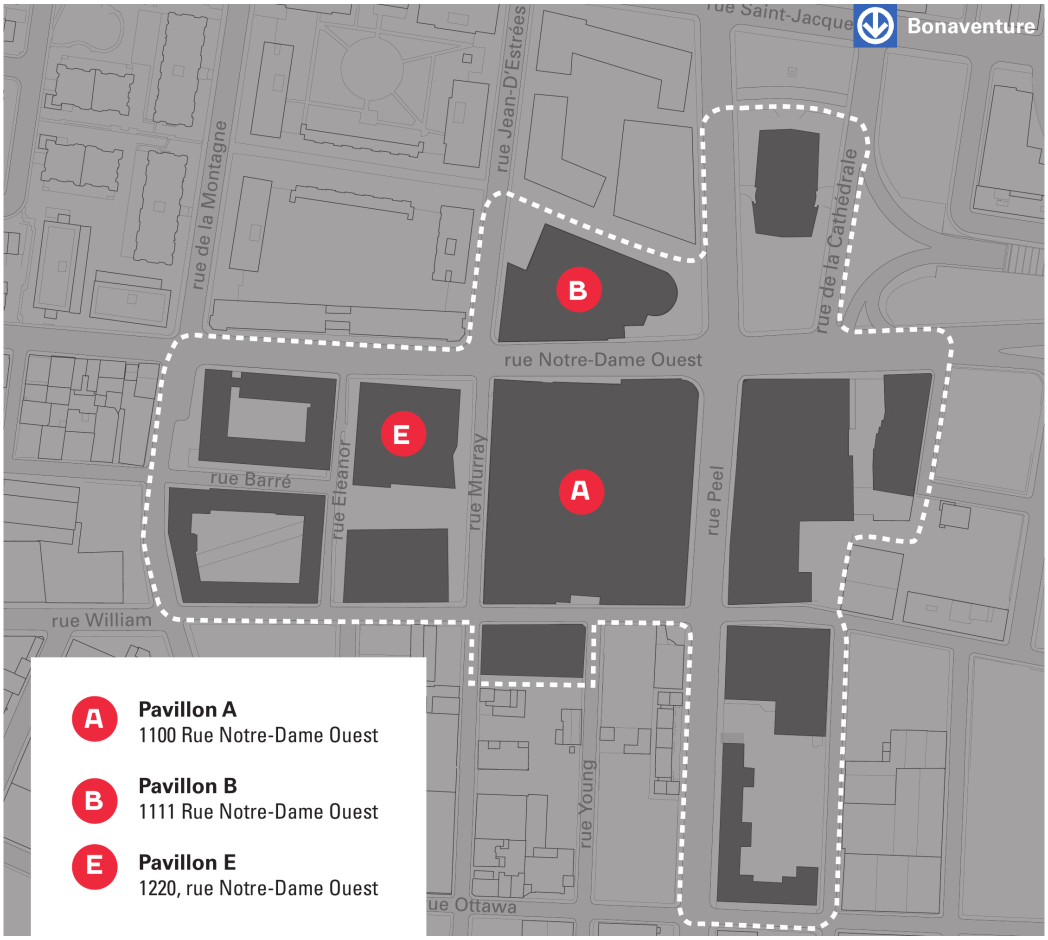
The ACA 2019 logo was designed by Loogart (`https://loogart.com/`) and is constituted of 6 distinctive elements:

- The Biosphere (former pavilion of the United States for the 1967 World Fair, Expo 67, designed by Buckminster Fuller)
- The Mont Royal (Montréal's iconic park designed by Frederick Law Olmsted, the highly skilled designer behind New York's Central Park)
- The Montréal Tower (tallest inclined tower in the world, rising 165 metres at a 45-degree angle)
- Habitat 67 (housing complex designed by Israeli-Canadian architect Moshe Safdie)
- ÉTS main building, Pavillon A (former Dow Brewery Bottling Plant)
- Digital wave signal (representing science, mathematics, engineering and computer science)

Maps

Campus

ACA 2019 is held on the campus of École de technologie supérieure (ÉTS) located at the corner of Notre-Dame Ouest and Peel streets in downtown Montreal. It is a 10-minute walk from Bonaventure metro station (rue de la Cathédrale exit).



Pavillon E

Main entrance and second floor
The registration desk is located on the ground floor next to the entrance. The poster session (E - 2010), the coffee breaks and the welcome reception with the Maplesoft booth (E-2011) are held in the Atrium of the second floor. The keynote lectures and the ACA Working Group meeting are hosted in the Salon des diplômés Vidéotron (E-2033).

⟵ rue Notre-Dame Ouest ⟶

Fourth floor

The conference rooms E-4024, E-4025 and E-4026 are located on the fourth floor.

← rue Notre-Dame Ouest →

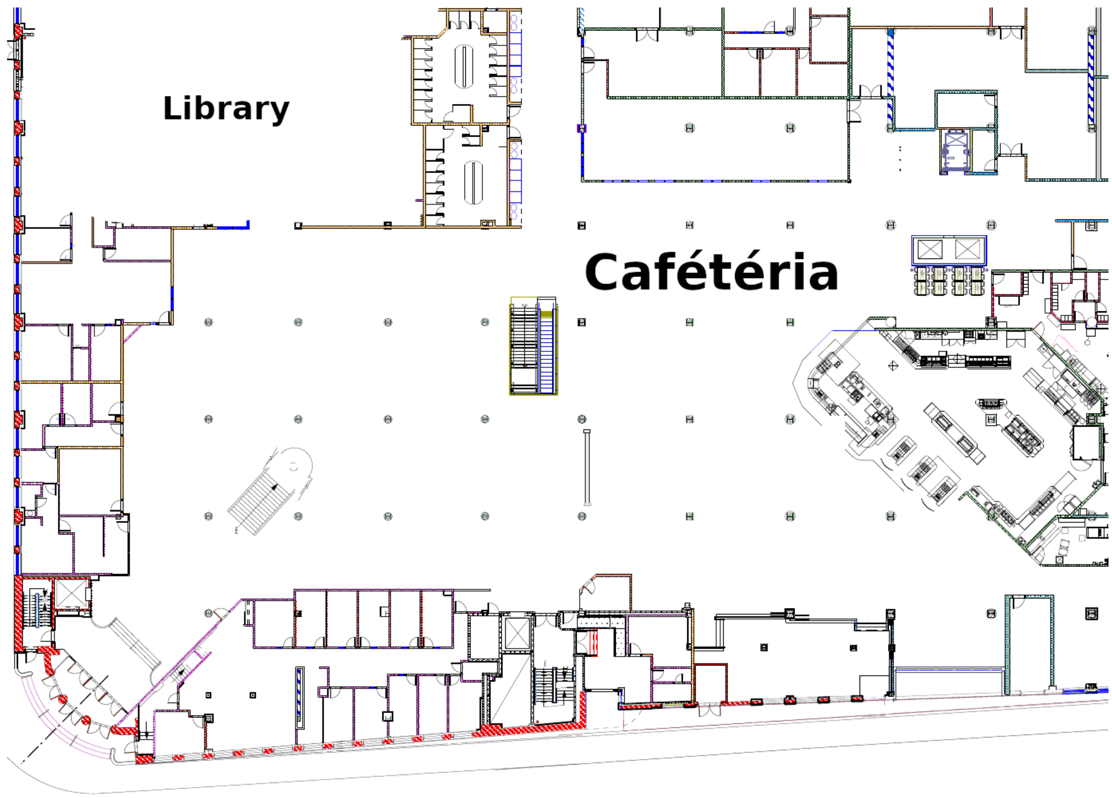
Pavillon B

The conference rooms B-0904 and B-0906 are located on the ground floor.

⟵ rue Notre-Dame Ouest ⟶

Pavillon A

The cafeteria is located on the ground floor. There is a dedicated lunch section for ACA attendees delimited with black curtains. The library is located across the main hall.



⟵ rue Notre-Dame Ouest ⟶

Social Activities

The ACA participants, as well as the registered accompanying persons, can enjoy three social activities included in the registration fees: the Welcome reception, the Excursion and the Banquet. There are two optional activities ($) where participants must purchase food and drinks.

Welcome reception

A Welcome Reception will be held on Tuesday, July 16, from 17:00 to 20:00 in the Atrium of Pavillon E (1220 rue Notre-Dame Ouest). The registration desk will be set up near the main entrance of Pavillon E. Delegates will be able to register and pick up their conference kit before attending the reception. Drinks and hors d'oeuvres will be served.

Excursion

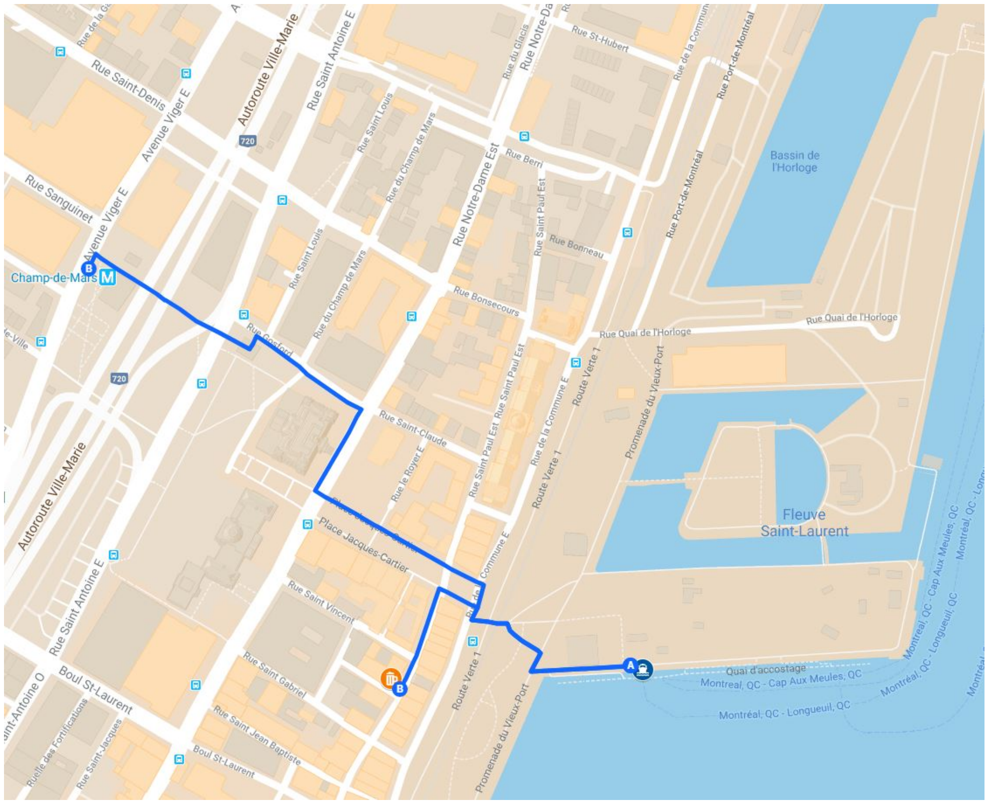
The excursion is scheduled after lunch on Thursday, July 18. Participants will meet by the main entrance of Pavillon E at 13:45. The buses will leave the campus at 14:00.

The excursion features a bus tour across the Monteregian Hills and a boat cruise on the Fleuve St-Laurent. The bus tour stops at Domaine de Lavoie for a cider and wine tasting activity with splendid views on Mont Rougemont. Participants will learn about the First Nations traditions with a guided visit of La Maison amérindienne located in Mont Saint-Hilaire.

After these two visits, the buses will bring the participants to the Longueuil Marina, on the south shore of Montréal. Participants can expect exquisite panoramic views of Montréal skyline during sunset while cruising their way back to Vieux-Montréal. A light meal will be served on the boat. Arrival in the Old Port of Montréal is expected at 21:00, which ends the excursion. To get back to your accommodation, the nearest transit option is the Champ-de-Mars metro station (orange line).

Wear comfortable walking shoes, bring water and a smile! :)

Optional late night drink ($)
The organizing committee invites all participants to share a last drink at 3 Brasseurs (105 rue St-Paul Est), a nearby pub in Vieux-Montréal. More information will be given on the boat.



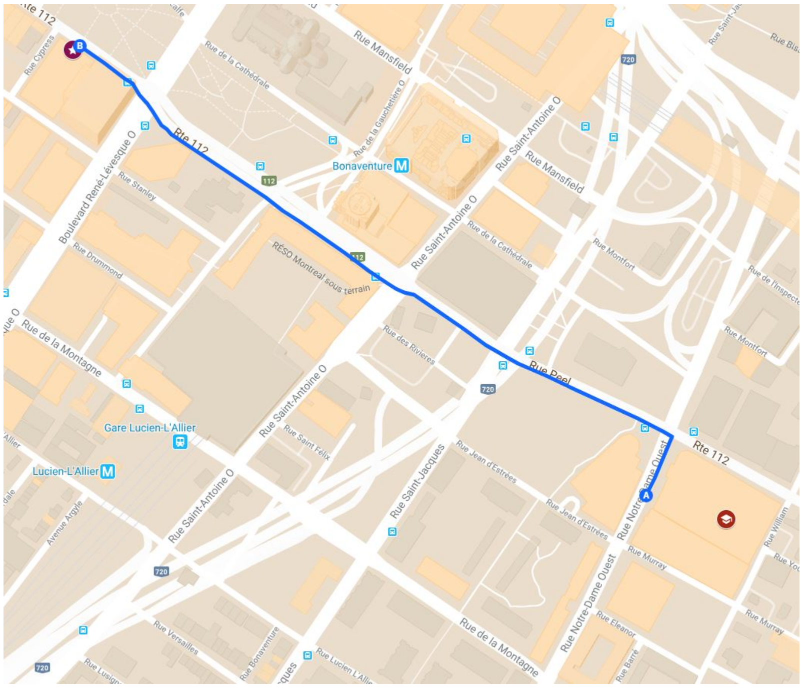
Vieux-Montréal : Itinerary from cruise arrivals to 3 Brasseurs and Champ-de-Mars metro station.

Banquet

The banquet dinner will be held on Friday, July 19, 2019 at Le Windsor Ballrooms located at 1170 rue Peel in front of Dorchester Square. It is a 15-minute walk from the ÉTS campus (1 km). **Be careful not to confuse Le Windsor with the old train station building La Gare Windsor located nearby!** Check the map below.

The cocktail preceding the banquet dinner will start at 19:00 in the Peacock Alley. The dinner will take place in the Versailles Ballroom.

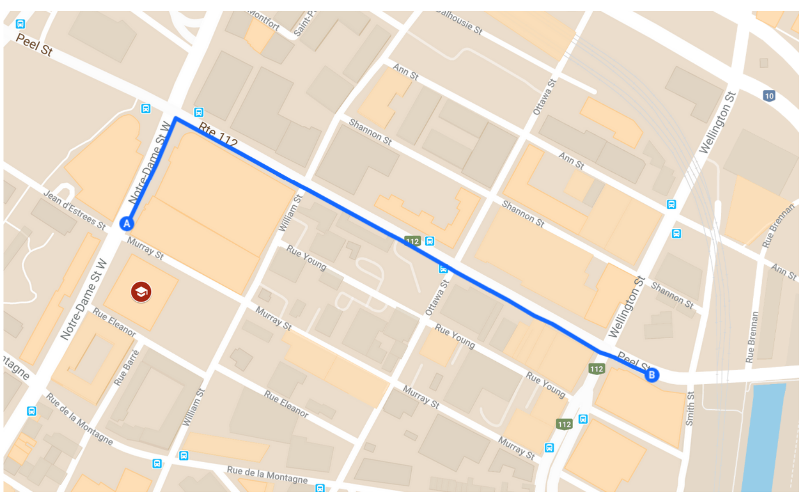
Vegetarian menus or menus for those with food allergies have been planned for all who have indicated such needs. Simply make yourself known to the staff. Be aware that special menus are available to you if and only if you mentioned it when registering for ACA 2019.



Itinerary from ÉTS campus to Le Windsor Ballrooms.

Closing ceremony ($)

The conference ends on Saturday, July 20 at 12:30. The organizing committee invites all participants to share one last meal at ZIBO!, a restaurant located at 90 rue Peel, a 10-minute walk from campus. Participants will gather in the Atrium (E-2011) at 12:30. The group will leave for the restaurant at 12:45.



Itinerary from ÉTS campus to ZIBO!.

Canadian Applied and Industrial Mathematics Society

Société Canadienne de Mathématiques Appliquées et Industrielles

CAIMS
SCMAI

Promoting and supporting applied and industrial mathematics in Canada since 1979.
Promotion et soutien des mathématiques appliquées et industrielles au Canada depuis 1979.

www.caims.ca

Mathematics in Science and Industry

is the official journal of CAIMS.
est le journal officiel de SCMAI.

Publish today!
Publier aujourd'hui!

CAIMS
SCMAI

Des outils numériques

pour renforcer l'autonomie et les apprentissages de vos étudiants, tout en vous faisant gagner du temps.

MonLab xL

LA PLATEFORME **SCIENCES**

Des exercices avec données aléatoires et correction automatisée pour renforcer les compétences des étudiants.

GeoGebra

LA VISUALISATION **DYNAMIQUE**

Des animations pour aider les étudiants à visualiser et à comprendre les concepts abstraits.

Pearson
ERPI

Canadian Mathematical Society
Société mathématique du Canada

Will you be there? | Y serez-vous?

CMS Meetings | Réunions de la SMC

The Canadian Mathematical Society (CMS) invites the mathematical community to the upcoming CMS Meetings. | La Société mathématique du Canada (SMC) invite la communauté mathématique à ses prochaines Réunions.

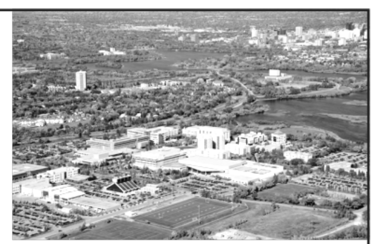
Highlights Include | Au programme :

- NEW: Mini Courses on Friday | NOUVEAU : Mini-cours le vendredi
- Over 20 Scientific Sessions | Plus de 20 sessions scientifiques
- Prestigious Plenary Lectures | Conférences plénières prestigieuses
- Student Activities | Activités étudiantes
- Public Lecture | Conférence publique

Save the Date! | Inscrivez cette date à votre agenda!

- **2019 CMS Winter Meeting | Réunion d'hiver 2019 de la SMC**
  December 6-9 décembre | Toronto
- **2020 CMS Summer Meeting | Réunion d'été 2020 de la SMC**
  June 5-8 juin | Ottawa
- **2020 CMS Winter Meeting | Réunion d'hiver 2020 de la SMC**
  December 4-7 décembre | Montréal

cms.math.ca | smc.math.ca



Schedule

Special Sessions

S1	Algebraic and Algorithmic Aspects of Differential and Integral Operators Session	E-4025
S2	Algebraic Geometry from an Algorithmic Point of View	E-4025
S3	Computational Differential and Difference Algebra and its Applications	E-4024
S4	Computer Algebra and Applications to Combinatorics, Coding Theory and Cryptography	E-4026
S5	Computer Algebra for Dynamical Systems and Celestial Mechanics	E-4024
S6	Computer Algebra in Education	B-0904
S7	Computer Algebra Modeling in Science and Engineering	E-4026 E-4024
S8	Proving and Discovery in Geometry: Dynamic Geometry, Computer Algebra and Mathematics Education	B-0906 E-4024
S9	Use of Mathematical Software in Research and Teaching through the Blending of CASs and DGS	B-0906

Poster Session

Thursday, 10:15 – 11:00, in the Atrium (Room E-2010)

	Tuesday July 16	Wednesday July 17	Thursday July 18	Friday July 19	Saturday July 20
8:30 – 9:00		Registration + Coffee	Coffee	Coffee	
9:00 – 9:30		Opening ceremony + Keynote presentation Simon Plouffe	Keynote presentation Sylvie Ratté	Maple + Keynote presentation David Stoutemyer	Coffee
9:30 – 10:00					Keynote presentation Franco Saliola
10:00 – 10:15			Group Photo (10:00 – 10:15)		
10:15 – 10:30			Poster session + Coffee break		
10:30 – 11:00		Coffee break		Coffee break	Coffee break
11:00 – 11:30		Parallel sessions	Parallel sessions	Parallel sessions	Parallel sessions
11:30 – 12:00		Parallel sessions	Parallel sessions	Parallel sessions	Parallel sessions
12:00 – 12:30		Parallel sessions	Parallel sessions	Parallel sessions	Parallel sessions
12:30 – 14:00		Lunch	Lunch	Lunch	Closing Ceremony
14:00 – 14:30		Parallel sessions	Excursion	Parallel sessions	
14:30 – 15:00		Parallel sessions		Parallel sessions	
15:00 – 15:30		Parallel sessions		Parallel sessions	
15:30 – 16:00		Coffee break		Coffee break	
16:00 – 16:30	Registration	Parallel sessions		Parallel sessions	
16:30 – 17:00		Parallel sessions		Parallel sessions	
17:00 – 17:30	Welcome reception (until 20:00)	Parallel sessions		ACAWG meeting	
17:30 – 18:00		Education session			
19:00 ++				Banquet (The Windsor)	

	Wednesday July 17				
8:30 – 9:00	**Registration + Coffee** **Room E-1012**				
9:00 – 10:30	**Opening ceremony** **+** **Keynote presentation** Simon Plouffe, *π, the primes and the Lambert W function* **Room E-2033**				
10:30 – 11:00	**Coffee break**				
	S6 Room B-0904	**S8 Room B-0906**	**S3 Room E-4024**	**S2 Room E-4025**	**S7 Room E-4026**
11:00 – 11:30	Gosia Brothers *Exciting Updates to the TI-Nspire™ World (Part I)*	Pedro Quaresma *Tracing the Evolution of Current Automatic Proving Technologies*	James Freitag *A computational method for the strong minimality of differential equations*	David Sevilla *Rational reparametrization of polynomial ODEs, PDEs and linear systems with radical coefficients*	Haiduke Sarafian *A Study of sensitivity of nonlinear oscillations of a CLD-series circuit to parametrization of tunnel diode*
11:30 – 12:00	Gosia Brothers *Exciting Updates to the TI-Nspire™ World (Part II)*	Peter Barendse and Daniel McDonald *Automated Plane Geometry in Wolfram Mathematica*	Vladimir Bavula *The generalized Weyl Poisson algebras and their Poisson simplicity criterion*	Gabriel Langeloh *Unrestricted dynamic Gröbner Basis algorithms*	Ali Bilek *Analysis and modeling of contact stresses between two deformable bodies*
12:00 – 12:30	William Bauldry and Wade Ellis *Dynamic Applications for Learning and Exploring Mathematics Using Computer Algebra*	Ludovic Font and Philippe R. Richard *The realization of a proof support system in a process of adaptation to the human perspective*	Alexander Levin *Hilbert-type Functions of Non-reflexive Prime Difference Polynomial Ideals*	Robert H. Lewis *New heuristics and extensions of the Dixon resultant for solving polynomial systems*	Salah Zouaoui *Towards the numerical simulation of fluid/solid particles flow inside a pipe*
12:30 – 14:00	**Lunch** **Cafétéria, Pavillon A**				
	S6 Room B-0904	**S8 Room B-0906**	**S3 Room E-4024**	**S2 Room E-4025**	**S7 Room E-4026**
14:00 – 14:30	Pauline Hubert *Interactive tutorials, an example on symmetric functions*	Nicolas Leduc and Pascal-Alexandre Morel *The Modelisation of the Possible Proofs for High School Geometry Problems in the Tutoring Software QED-Tutrix*	Richard Gustavson *Order bounds for differential elimination algorithms*	John Perry *A dynamic F3 algorithm*	Hassane Djebouri *Viscous fingering in five-spot immiscible displacement*
14:30 – 15:00	Helmut Heugl *Realizing the concept of "Multiple Representations" by using CAS (Part I)*	Thierry Dana-Picard *Experiments on isoptics by dynamic coloring*	Peter Thompson *A differential algebra approach to parameter identifiability in ODE models*	Teo Mora *Weak involutive bases over effective rings (Part I)*	Ionel Tifrea *Graphene transport in a parallel magnetic field: spin polarization effects at finite temperature*
15:00 – 15:30	Helmut Heugl *Realizing the concept of "Multiple Representations" by using CAS (Part II)*	Viktor Freiman *Rearrangement method for area of a circle: complex paths from historical roots to modern visual and dynamic models in discovery-based teaching approach*	Johann Mitteramskogler *A Maple package for solving algebraic differential equations by algebro-geometric methods*	Teo Mora *Weak involutive bases over effective rings (Part II)*	Avi Karsenty *Pre-manufacturing behavior forecasting and modeling of silicon photonics dual-mode devices using computer algebra*

	Wednesday July 17				
15:30 – 16:00	Coffee break				
	S6 Room B-0904	S8 Room B-0906	S3 Room E-4024	S2 Room E-4025	
16:00 – 16:30	Gilbert Labelle *Putting words on arrows and loops*	Alain Kuzniak *Vers un travail géométrique conforme et correct en contexte d'usages d'outils géométriques classiques et numériques*	Carlos Arreche *Differential transcendence of elliptic hypergeometric functions through Galois theory*	Martin Weimann *Computing the genus of plane curves with cubic complexity in the degree*	
16:30 – 17:00	Jan Krupa and Włodzimierz Wojas *Symbolic calculation behind floating-point arithmetic using CAS*	Jiří Blažek *Discovering in DGE — A case study*	Mengxiao Sun *On the Complexity of Computing the Galois Group of a Linear Differential Equation*	Michela Ceria *Bar Code and Janet-like division*	
17:00 – 17:30	Aharon Naiman *Gaussian Elimination with Parameters*	Roman Hašek *One method of trisecting an angle and its interpretation for teaching purposes using a dynamic geometry and computer algebra system*		Stephen M. Watt Algorithms for Polynomials in Legendre-Sobolev Bases	
17:30 – 18:00	Elena Varbanova *Methodological issues of application of computer algebra in blended learning environment*				

	Thursday July 18				
8:30 – 9:00	**Coffee**				
9:00 – 10:00	**Keynote presentation** Sylvie Ratté, *Looking under the hood of Artificial Intelligence: About cookies, blood, language, and some mathematics* **Room E-2033**				
10:00 – 10:15	**Group photo** **Room E-1012**				
10:15 – 11:00	**Poster session** Thanh-Trung Do, *Automatic Generation of Inverse Dynamics for Industrial Robots with Flexible Joints Using a Computer Algebra* Barry H. Dayton, *Software for Real Algebraic Curves In the Wolfram Language* Koissi Adjorlolo, *Manipulating Symbolic Expressions on a Computer* **Atrium (Room E-2010)** **+** **Coffee break**				
	S6 Room B-0904	**S9 Room B-0906**	**S8 Room E-4024**	**S2 Room E-4025**	**S4 Room E-4026**
11:00 – 11:30	Aharon Naiman *Proving and Disproving Subspaces with Mathematica*	Alexander Prokopenya *Animation of some mechanical systems with Mathematica*	Jean-Jacques Dahan *Investigations with DGS and CAS dealing with problems of equal area and particularly a possible generalization to 3D of the known results of the Lhuillier problem (Part I)*	Mark Huibregtse *Some new elementary components of the Hilbert scheme of points*	Pierre-Louis Cayrel *Code-based cryptography: from McEliece to the NIST competition*
11:30 – 12:00	Thierry Dana-Picard *Parametric integrals, combinatorial identities and applications*	Emmanuel Roque *Symbolical and numerical study of Fourier series and PDEs using Maxima*	Jean-Jacques Dahan *Investigations with DGS and CAS dealing with problems of equal area and particularly a possible generalization to 3D of the known results of the Lhuillier problem (Part II)*	Elisa Palezzato *Modular methods for rich algebraic geometry results on hyperplane arrangements*	Reza Dastbasteh *Constructions of quantum codes*
12:00 – 12:30	David Jeffrey and David Stoutemyer *The importance of being continuously continuous*	Setsuo Takato *Development and Applications of KeTCindyJS*		Cristina Bertone *On algebraic and geometric properties of almost revlex ideals*	Malihe Aliasgari *Distributed Coded Computation*
12:30 – 14:00	**Lunch** **Cafétéria, Pavillon A**				
14:00 – 21:00	**Excursion**				

	Friday July 19				
8:30 – 9:00	**Coffee**				
9:00 – 10:30	**Maple presentation** **+** **Keynote presentation** David Stoutemyer, *The Constant hunters* **Room E-2033**				
10:30 – 11:00	**Coffee break**				
	S6 Room B-0904	**S9 Room B-0906**	**S7 Room E-4024**	**S1 Room E-4025**	**S4 Room E-4026**
11:00 – 11:30	Paulina Chin *Assessment Tools in Maple: Recent Developments and Challenges*	Yoichi Maeda *Three-dimensional model of SL(2,R) and visualization of SL(2,Z) as a pattern on the cubic lattice*	Ryszard Kozera *Reparametrizations and Lagrange piecewise-cubics for fitting reduced data*	Maximilan Jaroschek *First order differential and difference systems in Sage*	Theo Moriarty *Why you cannot even hope to use Gröbner bases in cryptography: an eternal golden braid of failures*
11:30 – 12:00	Thierry Dana-Picard *DGS assisted activities around the Golden Ratio in Space and Time*	Tetsuo Fukui *Educational graph creation tool based on the natural mathematical description*	Alexander Prokopenya *Dynamics of a generalized Atwood's machine with three degrees of freedom*	Alexander Levin *Some properties and applications of multivariate dimension polynomials and their computation in Python*	Michela Ceria *HELP: the knight gambit for efficient decoding of BCH codes*
12:00 – 12:30	M. Pilar Vélez *GeoGebra Automated Reasoning Tools: a problem from Spanish Civil Service Math Teachers' examination*	Tatiana Mylläri *Fractals in the classroom with CAS and KeTCindy*	Alexander Prokopenya *Analytical calculations of secular perturbations of translational-rotational motion of a non-stationary triaxial body in the central field of attraction*	Franz Winkler *A decision algorithm for strong rational general solutions of algebraic ordinary differential equations*	Madhu Raka *Skew constacyclic codes over a non-chain ring*
12:30 – 14:00	**Lunch** **Cafétéria, Pavillon A**				
	S6 Room B-0904	**S9 Room B-0906**	**S7 Room E-4024**	**S1 Room E-4025**	**S4 Room E-4026**
14:00 – 14:30	José Luis Galán-García *Teaching the residue theorem and its applications with a Cas*	Naoki Hamaguchi *A teaching material for orthogonal transformations using rotation of cuboids*	Jose A. Vallejo *Mathematical modelling with Fourier series and PDEs*	Vladimir Bavula *Localizable sets and the localization of a ring at a localizable set*	Daniel J. Katz *Rudin-Shapiro-like sequences with low correlation*
14:30 – 15:00	Jan Krupa and Włodzimierz Wojas *Some examples of calculation improper integrals using CAS*	Koji Nishiura *Effective Use of KeTCindy in an Experimental Study to Develop Methods of Teaching Mathematics*	Setsuo Takato *Producing animations of some physical phenomena with KeTCindy*	Cyrille Chenavier *An effective version of Warfield's theorem*	Mercè Villanueva *PD-sets for partial permutation decoding of Z_2^s-linear Hadamard codes*
15:00 – 15:30	Gabriel Aguilera-Venegas *Using a CAS-developed random samples generator for teaching and researching in probabilistic cellular automata and Statistics*	Takeo Noda *Visualizing ODEs with KeTCindy*	Haiduke Sarafian *A two-dimensional nonlinear oscillator in a charged rectangular frame*	Ruyong Feng and Ziming Li *Telescopers for differential forms with one parameter*	Curtis Bright *Searching for projective planes with computer algebra and SAT solvers*

	Friday July 19				
15:30 – 16:00	**Coffee break**				
	S6 Room B-0904	**S9 Room B-0906**	**S5 Room E-4024**	**S1 Room E-4025**	**S4 Room E-4026**
16:00 - 16:30	Michael Xue *Boosting Rocket Performance without Calculus*	Tomoya Tokairin *Extension of KeTCindyJS to generate interactive HTML slides*	Anna Myullyari *On the complexity of finite sequences*	Thomas Cluzeau *An efficient algorithm for the simultaneous triangularization of a finite set of matrices*	Simon Eisenbarth *Relative projective group ring codes over chain rings*
16:30 – 17:00	José Luis Galán-García *SFOPDES.dfw: A stepwise tutorial for solving Partial Differential Equations with Derive*	Satoshi Yamashita *Calculation and visualization of Fourier series with KeTCindy and KeTCindyJS*	Aleksandr Mylläri *On the dynamical system generated by the three-body integrator*	Sette Diop *Towards a differential algebraic decision methods toolbox for systems theory*	Kenza Guenda *Errors correcting codes over rings*
17:00 – 17:30	**ACA Working Group Meting Room E-2033**				
19:00 ++	**Banquet The Windsor, 1170 Peel street**				

	Saturday July 20		
9:00 – 9:30	**Coffee**		
9:30 – 10:30	**Keynote presentation** Franco Saliola, *Computer Exploration in Algebraic Combinatorics via SageMath* **Room E-2033**		
10:30 – 11:00	**Coffee break**		
	S6 Room B-0904	**S5 Room E-4024**	**S1 Room E-4025**
11:00 – 11:30	Daniel Jarvis *Innovative CAS Technology Use in University Mathematics Teaching and Assessment*	Ariel Chitan *Influence of Relativistic Effects on the Evolution of Triple Black Hole Systems*	Mark van Hoeij *Factoring linear recurrence operators*
11:30 – 12:00	Karsten Schmidt *Teaching Decision Analysis using a Computer Algebra System*		Johannes Middeke *A direct solver to find hypergeometric solutions for coupled systems of difference equations*
12:00 – 12:30	Jan Krupa and Włodzimierz Wojas *Familiarizing students with definition of Lebesgue integral using Mathematica - some examples of calculation directly from its definition: Part 2*		Clemens Raab *On rational solutions of linear systems of Mahler equations*
12:30	**Closing Ceremony** **Atrium (Room E-2011)**		

Invited Speakers

π, the primes and the LambertW function

Simon Plouffe[1] [simon.plouffe@gmail.com]

[1] Université de Nantes (IUT), Nantes, France

The talk is divided into two parts, the first part will show how to use the bootstrap method to get a formula to calculate the arguments of $\zeta\left(\frac{1}{2}+in\right)$ and a spectacular formula for the n'th zero of the Zeta function using Lambert$W$ function.

The second part will show new formulas for primes like

$$691 = 2^4 \sum_{n=1}^{\infty} \frac{n^{11}}{e^{n\pi}-1} - 2^{16} \sum_{n=1}^{\infty} \frac{n^{11}}{e^{4n\pi}-1}$$

At the same time, the prime 691 is well approximated with the formula

$$691 \approx \frac{2^4 11!}{\pi^{12}}$$

In fact, the prime 691 is given exactly by

$$691 = \frac{2^4 11!}{\pi^{12}} \left(1 + \frac{1}{3^{12}} + \frac{1}{5^{12}} + \frac{1}{7^{12}} + \dots\right)$$

Using the bootstrap method, one can do the same for many primes. This leads to a conjecture about the representation of all the primes using π and a simple function of n. And speaking of primes, I will show a set of formulas that can generate an infinity of primes using a recurrence equation function. If $\{x\}$ is the rounded value of x and $S_0 = 43.804\dots$, then $S_{n+1} = \left\{S_n^{5/4}\right\}$ will generate an infinity of primes, beginning with

$$113, 367, 1607, 10177, 102217, 1827697, 67201679, 6084503671, \dots$$

Here, the exponent 5/4 can be made as close as we want to 1.

Looking under the hood of Artificial Intelligence:
About cookies, blood, language, and some mathematics

Sylvie Ratté[1] [sylvie.ratte@etsmtl.ca]

[1] LiNCS & LiVE Labs, Software and IT Engineering Department,
École de technologie supérieure, Canada

What does the little girl is asking to the little boy that he took from a jar on a shelf in the kitchen while his mother is washing dishes unaware that the sink is overflowing? And, while I am at it, what is this little twisted tube moving weirdly with a wire inside that suddenly disappear out of view provoking great despair for those who were looking?

The first sentence of this abstract describes a common test used to detect dementia and the answer is in the title of this presentation. The second one is the partial description of a cardiac catheterization surgery on newborns using contrast agent. These two sentences themselves are also quite obvious examples of why it is still difficult for computers to understand natural languages (although I am sure you struggled a bit too). They are also examples of two research projects using Artificial Intelligence (AI).

Where are the mathematics? They are, of course, under the hood of AI, and its application to solve these problems here at ÉTS. I don't want to sell the punchline so I will throw at you two images and two formulas here.

$$Coverage(R,S) = \frac{\sum_{p \in \{R\}} \alpha_p MaxSim(p,S)}{\sum_{p \in \{R\}} \alpha_p} \tag{1}$$

Formula (1) (taken from [1]) is an asymmetric coverage measure (inspired by [2]) used to distinguish the discourses of patients during the "Cookie Theft Picture Description Task" [3]. *MaxSim* is a function that measures the similarity between a referent, R (healthy population) and a subject, S (with cognitive decline). The parameters α_p are used to associate a weight to each simplified linguistic pattern, p, that we identified as relevant for the task.

Figure 1 illustrates a Principal Component Analysis (components 1 and 3) of patients' discourses evolving through time (10 years). The label near each point indicates the participant ID-interview number. Interviews 1, 2 and 3 were held in 2005, 2012 and 2015, respectively (see [5, 6] for the data). The hue difference indicates normal or cognitively declined aging processes. Circle, square and rhomboid markers indicate healthy control (HC), mild cognitive impairment (MCI) and severe CI, respectively, at the time of the interview.

$$C_n = \frac{1}{n+1}\binom{2n}{n} \tag{2}$$

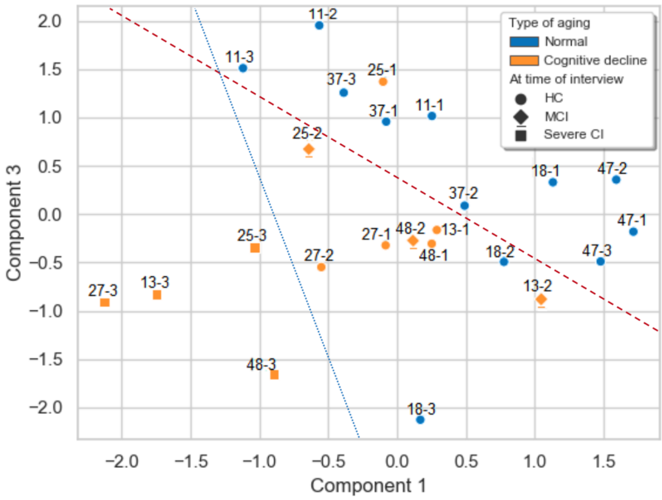


Figure 1: Patients' discourses evolving through time [4]

Formula (2) points to the well-known difficulty of analyzing symbolically natural languages by associating binary trees to sentences (= parsing trees). On this account (presented in [7] for natural languages), our first sentence can theoretically produce an extravagant number of syntactic trees; while humans discard most of them without even thinking, computers find the task phenomenally troublesome.

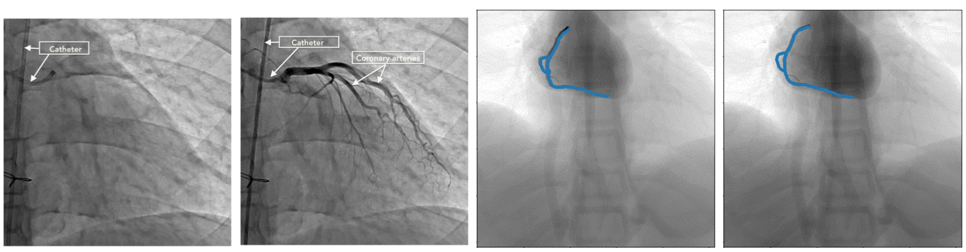


Figure 2: Left: X-ray frame without (1) and with (2) contrast agent (from [8]). Right: Tracking of cardiac artery during movement (from [9]).

Finally, figure 2 illustrates the challenges of tracking coronary arteries to help surgeons during cardiac catheterization. There are two challenges here. First, as in the case of sentences analysis, you must be able to recognize the real vessel within the noise surrounding it (two figures on the left, from [8]). Second, the patient is breathing and his heart is beating (hopefully!), so that twisted tube is moving (two figures on the right, from [9]).

My intention is to use these applications to introduce you to natural language processing and machine learning. We will finish our journey pointing to a sample of research themes related to AI at ÉTS, and why education in mathematics and ethics is so important in this new world obsessed with AI.

Keywords
Artificial Intelligence, Matrix algebra, Neural networks, Natural language processing, Medical image processing

References

[1] L. Hernández-Domínguez, S. Ratté, G. Sierra-Martínez, A. Roche-Bergua, Computer-based evaluation of Alzheimer's disease and mild cognitive impairment patients during a picture description task. *Alzheimer's & Dementia: Diagnosis, Assessment & Disease Monitoring* **10**, 260–268 (2018).
[2] E. Velázquez-Godínez, *Caractérisation de la couverture d'information : Une approche computationnelle fondée sur les asymétries*. Ph.D. Thesis, École de technologie supérieure, 2017.
[3] O. Spreen, A.H. Risser, *Assessment of aphasia*. Oxford University Press, 2003.
[4] L. Hernández-Domínguez, S. Ratté, A. Gerstenberg, G. Sierra-Martínez, Aging with and without cognitive diseases: Characterizing 10 years of language differences in older French speakers. *Computer Speech and Language* (under review).
[5] A. Gerstenberg, *LangAge Collection of Biographical Interviews*. University of Potsdam: Department of Romance Studies, www.langage-corpora.org (2005-).
[6] A. Gerstenberg, Generation und Sprachprofile im höheren Lebensalter: Untersuchungen zum Französischen auf der Basis eines Korpus biographischer Interviews. *Analecta Romanica* **76**. Frankfurt am Main: Vittorio Klostermann (2011).
[7] K. Church, R. Patil, Coping with syntactic ambiguity or how to put the block in the box on the table, *Computational Linguistics* **8**(3–4), 139–149.(1982).
[8] F. Mhiri, *Angiographic image analysis for the diagnosis of coronary disease in young patients*. Ph.D. Thesis, École de technologie supérieure, 2016.
[9] F. Azizmohammadi, R. Martin, M.J. Miro, L. Duong, Model-free cardiorespiratory motion prediction from X-ray angiography sequence with LSTM network. In *41st International Engineering in Medicine and Biology Conference*, 6 p. IEEE, Berlin, 2019.

Computer exploration in Algebraic Combinatorics via SageMath

Franco Saliola[1] [saliola.franco@uqam.ca]

[1] Laboratoire d'Algèbre, de Combinatoire, et d'Informatique Mathématique (LACIM)
Département de mathématiques, Université du Québec à Montréal (UQAM), Canada

This talk is divided into two parts. The first will be an introduction to the SageMath project from a personal perspective. From the SageMath website:

> **SageMath** is a free open-source mathematics software system licensed under the GPL. It builds on top of many existing open-source packages: NumPy, SciPy, matplotlib, Sympy, Maxima, GAP, FLINT, R and many more. Access their combined power through a common, Python-based language or directly via interfaces or wrappers.
>
> Mission: *Creating a viable free open source alternative to Magma, Maple, Mathematica and Matlab.*

SageMath has become an essential tool in my field of research, algebraic combinatorics. The scope of algebraic combinatorics has grown so much as to encompass any area of mathematics "where the interaction of combinatorial and algebraic methods is particularly strong and significant" [Wikipedia]. This significant interaction between combinatorics and algebra is what makes many of the problems in this field amenable to computer exploration.

The first part of this talk will focus on the history and some features of the SageMath project. The second part will highlight a few examples of how computer exploration is used as a research tool in algebraic combinatorics.

The Constant hunters

David R. Stoutemyer[1] [dstout@hawaii.edu]

[1] University of Hawaii, UNITED STATES

There are now several comprehensive programs that, given a floating point number such as 6.518670730718491, can return concise non-float constants such as $3\arctan 2 + \ln 9 + 1$ that closely approximate the float. Surprisingly often such a result is the exact limit that is approached as the float is computed with increasing precision. Therefore these program results are candidates for proving an exact result that you could not otherwise compute or conjecture without the program. Moreover, candidates that are *not* the exact limit can be provable bounds, or convey qualitative insight, or suggest series that they truncate, or provide sufficiently close efficient approximations for subsequent computation.

1. Some such programs can be used freely online. For example:
   - **Inverse Symbolic Calculator** by Simon Plouffe, Jon and Peter Borwein, *et al*,
   - **Wolfram|Alpha**,
   - **On-line Encyclopedia of Integer Sequences** by Neil Sloane and Simon Plouffe.
2. Other such programs are *functions* built into a computer algebra system. For example:
   - the Maple **identify** function adapted by Kevin Hare from Alan Meichsner's M.S. thesis,
   - the **identify** and **findpoly** functions in MPMath, hence also SymPy and Sage.
3. Other such programs are freely downloadable. For example:
   - **Plouffe's inverter** Maple program,
   - the Java **MESearch** program developed by Jon Zurutuza Salsamendi,
   - the C **ries** program developed by Robert Munafo,
   - the *Mathematica* **AskConstants** program developed by me.

The presentation will demonstrate some of these programs and describe their varied underlying algorithms. Almost everyone who uses or should use mathematical software can benefit from acquaintance with several such programs, because these programs differ in the types of constants that they can return.

Special Sessions

S1 - Algebraic and Algorithmic Aspects of Differential and Integral Operators Session

Localizable sets and the localization of a ring at a localizable set

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

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

The concepts of localizable set, localization of a ring and a module at a localizable set are introduced and studied. Localizable sets are generalization of Ore sets and denominator sets, and the localization of a ring/module at a localizable set is a generalization of localization of a ring/module at a denominator set.

Keywords
Localizable set, localization of a ring at a localizable set, Goldie's Theorem, the left quotient ring of a ring, the largest left quotient ring of a ring, a maximal localizable set, a maximal left denominator set, the left localization radical of a ring.

References
[1] V. V. BAVULA, *Localizable sets and the localization of a ring at a localizable set*, submitted.

Telescopers for differential forms with one parameter

Shaoshi Chen[1] , **Ruyong Feng**[1] , **Ziming Li**[1] ,
Michael F. Singer[2] , **Stephen Watt**[3] [ryfeng@amss.ac.cn]

[1] KLMM, AMSS, Chinese Academy of Sciences, China
[2] North Carolina State University, USA
[3] University of Waterloo, Canada

Parallel telescopers introduced in [1] can be regarded as telescopers for differential 1-forms. In this talk, we generalize the results in [1] into differential p-forms. Precisely, let

$$\omega = \sum f_{i_1,\cdots,i_p} dx_{i_1} \wedge dx_{i_2} \wedge \cdots \wedge dx_{i_p}$$

be a differential p-form, where $f_{i_1,\cdots,i_p}$ is D-finite over $k(x_1,\cdots,x_n,t)$. A nonzero operator $L \in k(t)[\partial_t]$ is called a telescoper for ω if $L(\omega) = d\eta$ for some differential $p-1$-form η. We present a sufficient and necessary condition for a given differential p-form having a telescoper and develop an algorithm to compute a telescoper if it exists. We also give an algorithm to decide whether a given differential p-form has a telescoper or not.

Keywords
telescoper, differential form.

References

[1] R. Feng; S. Chen; Z. Li; M.F. Singer, Parallel Telescoping and Parametrized Picard-Vessiot Theory. *Proc. ISSAC2014*, July 23-25, Kobe, Japan, 99-104, ACM Press, 2014.

An effective version of Warfield's theorem

Cyrille Chenavier[1] [cyrille.chenavier@inria.fr]

[1] Inria Lille - Nord Europe, Villeneuve d'Ascq, France

A linear multidimensional system of q equations with p unknown functions $\eta_1, \cdots, \eta_p$ maybe described by a matrix $R \in D^{q\times p}$ as follows:

$$\ker_{\mathscr{F}}(R.) := \left\{\eta \in \mathscr{F}^p \mid R\eta = 0\right\}, \tag{1}$$

where $\mathscr{F}$ is the functionnal space where we are looking for the solutions. The latter admits a structure of *left D-module*, which enables us to described the space of solutions in terms of module theory: $\ker_{\mathscr{F}}(R.) \simeq \hom_D(M, \mathscr{F})$, where $M = D^{1\times p}/(D^{1\times Q}R)$ is the left D-module *finitely presented* by the matrix R. Under this point of view, some structural properties of (1) can be studied by mean of algebraic invariants. In particular, the formal manipulation of the system, such as exchange lines, multiply lines by a constant, lead to study the links between matrix conjugation and module isomorphisms. A result due to Fitting [2], asserts that two matrices presenting isomorphic left D-modules can be enlarged by blocks of 0 and identities to get equivalent matrices. A result due to Warfield [3] asserts that the number of 0 and identity blocs in the result of Fitting maybe reduced, the resulting matrices are still equivalent. This reduction procedure is based on the properties of the *stable rank* of D. The purpose of this talk is to provide an effective version of the Warfield's result. For that, we begin with the effective version of Fitting's result given in [1], and we use the stable rank for reducing the number of 0 and identity blocs.

Keywords
Module isomorphisms, equivalent matrices, stable rank

References

[1] T. CLUZEAU; A. QUADRAT, *A constructive version of Fitting's theorem onisomorphisms and equivalences of linear systems*, Proceedings of nDS'11, Poitiers, France, 2011.
[2] H. FITTING, Über den Zusammenhang zwischen dem Begriff der Gleichartigkeit zweier Ideale und dem Äquivalenzbegriff der Elementarteilertheorie, *Mathematische Annalen.* **112**(1), 572–582 (1936).
[3] R.B. WARFIELD, Stable equivalence matrices and resolution, *Communications in Algebra.* **6**(17), 1811–1828, (1978).

An efficient algorithm for the simultaneous triangularization of a finite set of matrices

***Moulay Barkatou*[1] , *Thomas Cluzeau*[1]** [thomas.cluzeau@unilim.fr]

[1] University of Limoges ; CNRS ; XLIM UMR 7252 ; MATHIS, 123 avenue Albert Thomas, 87060 Limoges, France

In the study of linear differential systems, one can be interested in deciding whether a set of m given square matrices $A_1, \ldots, A_m$ are simultaneously triangularizable or not. If the answer is yes, then we sometimes need to compute effectively an invertible matrix P such that, for all $i \in \{1, \ldots, m\}$, the matrix $P^{-1} A_i P$ is upper triangular. See, for instance, the recent paper [1].

The classical approach consists in using Lie algebra theory to test whether the matrix Lie algebra spanned by the A_i's is solvable (e.g., using the so-called derived series) and if so, find a basis in which all matrices of the Lie algebra are upper triangular using a constructive version of Lie's theorem on solvable algebras for computing common eigenvectors. See [2].

In this presentation, we will rather consider the following result due to McCoy [4]: matrices $A_1, \ldots, A_m$ are simultaneously triangularizable if and only if, for every scalar polynomial $p(x_1, \ldots, x_m)$ in the (non-commutative) variables $x_1, \ldots, x_m$, each of the matrices

$$p(A_1, \ldots, A_m)[A_i, A_j] = p(A_1, \ldots, A_m)(A_i A_j - A_j A_i) \quad (i, j = 1, \ldots, m)$$

is nilpotent. We shall show that the proof of this result provided in [3] can be turned into an efficient algorithm for computing particular common eigenvectors of $A_1, \ldots, A_m$. As a consequence, this yields an efficient algorithm for the simultaneous triangularization problem. Note that this new approach does not require the construction of the Lie algebra spanned by the matrices A_i's. The algorithm has been implemented in Maple and we will show comparisons to the implementation of the "Lie algebra method" included in the `DifferentialGeometry/LieAlgebras` package of Maple.

Keywords
computer algebra, algorithms, linear algebra, Lie algebras

References
[1] Barkatou M. A., Gontsov R., *Linear differential systems with small coefficients: various types of solvability and their verification.* https://arxiv.org/abs/1901.09951
[2] De Graaf W. A., *Lie Algebras: Theory and Algorithms.* Volume 56 of North-Holland Mathematical Library. Elsevier (2000).
[3] Drazin M. P., Duugey J. W., Gruenberg K. W., *Some theorems on commutative matrices.* J. London Math. Sot. 26: 221–228 (1951)
[4] McCoy N. H., *On the characteristic roots of matric polynomials.* Bull. Amer. Math. Sot. 42: 592-600 (1936)

Towards a differential algebraic decision methods toolbox for systems theory

Sette Diop[1] [Diop@L2S.CentraleSupelec.fr]

[1] L2S, CNRS, Gif sur Yvette, France

In last decades some systems theory questions have received differential algebraic partial answers. Among them obtaining input-output equations describing a system from its state space equations. This has been identified as a direct application of elimination theory, and Seidenberg seminal paper [2] has been one of the first differential algebraic decision methods which found its use in questions which are crucial in some areas of systems theory, namely, identification of systems parameters. Another important question of systems theory received a quite decent partial answer: observability and some related other observation problems occuring in systems design practice. The differential algebraic approach of this class of systems theory lead to decision methods stemming from the works of Ritt [1] and Kolchin [3]. In this contribution the previous two systems questions as well as others with differential algebraic decision methods partial answers are presented as building blocks of a toolbox for users who may not be familiar with the differential algebraic geometry machinery which underlies them.

Keywords
Differential algebraic decision methods, Systems theory, Control theory

References

[1] J. F. Ritt, *Differential Algebra.* American Mathematical Society, Providence, RI, 1950.
[2] A. Seidenberg, An elimination theory for differential algebra. *Univ. California Publ. Math. (N.S.)* **3**(2), 31–65 (1956).
[3] E. R. Kolchin, *Differential Algebra and Algebraic Groups.* Academic Press, New York, 1973.

First Order Differential and Difference Systems in Sage

Maximilian Jaroschek[1] [maximilian@mjaroschek.com]

[1] TU Wien, Institute for Logics and Computation, Favoritenstr. 9–11,1040 Wien, Austria.
Supported by the Austrian Science Fund (FWF) grant P 31427-N31.

We present a new package that provides users with the necessary tools to work with first order linear difference and differential systems in the computer algebra system `Sage` [2]. In its first version, the package under the tentative name `FOS` [1] supports many essential features for differential and difference systems in one variable, including computation of polynomial, rational, and formal solutions, super-reduction, desingularization, conversion to scalar equations, and more. We give a tutorial on how to use the package and show its capabilities in several examples.

Keywords
Systems of differential equations, systems of difference equations, Sage

References
[1] M. Jaroschek, FOS. `http://www.mjaroschek.com/fos/`
[2] The Sage Developers, SageMath, the Sage Mathematics Software System. `http://www.sagemath.org`

Some properties and applications of multivariate dimension polynomials and their computation in Python †

***Alexander Evgrafov*[1], *Sparsh Goyal*[2], *Alexander Levin*[3]** `[levin@cua.edu]`

[1]Department of Analytical, Physical and Colloid Chemistry, Sechenov First Moscow State Medical University, Moscow, Russia
[2]Department of Electrical Engineering and Computer Science, The Catholic University of America, Washington, DC, USA
[3] Department of Mathematics, The Catholic University of America, Washington, DC, USA

In this presentation we consider Hilbert-type polynomials in several variables that characterize finitely generated differential modules, that is, modules over rings of differential operators over differential fields. Such a polynomial describes the dimensions of components of a natural p-dimensional filtration ($p \geq 2$) associated with a system of generators of the module and a partition of the basic set of derivations into p subsets. Multivariate dimension polynomials of differential modules were introduced in [3] where their existence was established with the use of the technique of characteristic sets. The results of this work were essentially improved in [4] where one can find methods of computation of multivariate dimension polynomials via constructing generalized Gröbner bases (i. e., Gröbner bases with respect to several term orderings) in free differential modules. This approach was extended in [5] and [1] where the authors introduced a concept of relative Gröbner bases (Gröbner bases with respect to two generalized term orderings) and applied it to the computation of bivariate difference-differential dimension polynomials. There are also several recent works with similar results on multivariate dimension polynomials of difference and inversive difference modules.
The main results of our talk are as follows. We present algorithms for computing generalized Gröbner bases in free differential modules and for computing multivariate differential dimension polynomials, as well as implementations of these algorithms in Python. We also present some conditions under which a multivariate differential dimension polynomial has a special simple form. The obtained results are applied to the computation of differential dimension polynomials associated with the advection-diffusion equation and PDEs that arise in mathematical models of ion exchange chromatography studied in [2].

Keywords
Differential field, Differential module, Generalized Gröbner basis, Differential dimension polynomial

References

[1] C. DÖNCH; F. WINKLER, Bivariate difference-differential dimension polynomials and their computation in Maple. *Proceedings of the 8th International Conference on Applied Informatics*, Eger, 211–218 (2010).

†This work was supported by the NSF grant CCF-1714425

[2] A. A. EVGRAFOV, Standardization and control of the quality of transfusion liquids. *Ph. D. Thesis. Sechenov First Moscow State Medical University* (1998).
[3] A. B. LEVIN, Generalized characteristics sets and multivariable differential dimension polynomials. *Collections of Papers of VI International IMACS Conference on Applications of Computer Algebra*, St. Petersburg, 69–72 (2000).
[4] A. B. LEVIN, Gröbner bases with respect to several orderings and multivariable dimension polynomials. *Journal of Symbolic Computation* **42**(5), 561–578 (2007).
[5] M. ZHOU; F. WINKLER, Computing difference-differential dimension polynomials by relative Gröbner bases in difference-differential modules. *Journal of Symbolic Computation* **43**(10), 726–745 (2008).

A direct solver to find hypergeometric solutions for coupled systems of difference equations

***Moulay Barkatou*[1], *Johannes Middeke*[2], *Carsten Schneider*[2], *Mark van Hoeij*[3]** [jmiddeke@risc.jku.at]

[1] Université de Limoges, XLIM, 123, Av. A. Thomas, 87060 Limoges cedex, France
[2] Research Institute for Symbolic Computation (RISC), Johannes Kepler University, Altenbergerstraße 69, 4040 Linz, Austria
[3] Department of Mathematics, Florida State University, Tallahassee, FL 32306, USA

We are looking for hypergeometric solutions of first order linear recurrence systems $\tau(Y) = MY$ where τ is a forward shift operator and M is a square invertible matrix with rational function entries. Our approach aims at reducing this problem to the computation of polynomial solutions of certain related first order linear systems similarly to Petkovšek's algorithm [1]. In particular, we want to avoid uncoupling the system.

Keywords
recurrence systems, direct solving, hypergeometric solutions

References

[1] M. PETKOVŠEK, Hypergeometric solutions of linear recurrences with polynomial coefficients. *Journal of Symbolic Computation* (14), 243–264 (1992).

On rational solutions of linear systems of Mahler equations

Moulay A. Barkatou [1] **,** ***Clemens G. Raab*** [2] [clemens.raab@jku.at]

[1] Université de Limoges, CNRS XLIM UMR 7252, Limoges, France
[2] Inst. f. Algebra, Johannes Kepler Universität Linz, Linz, Austria

Mahler equations relate a function to its evaluation at certain powers of its argument. They arise in transcendence proofs and in the context of automatic sequences, for instance. In recent years, Mahler equations have received increasing attention, with both theoretical aspects and solution methods being investigated, see e.g. [1–4].

We report on ongoing work on algorithms for computing all rational function solutions of linear systems of Mahler equations. The presentation focuses on the computation of universal denominators for solutions of a given system. Our preliminary results will be illustrated by examples.

Keywords
Mahler equations, rational solutions, universal denominators

References

[1] B. Adamczewski; C. Faverjon, Méthode de Mahler, transcendence et relations linéaires: aspects effectifs. *J. Théor. Nombres Bordeaux* **30**, 557–573 (2018).
[2] F. Chyzak; T. Dreyfus; P. Dumas; M. Mezzarobba, Computing solutions of linear Mahler equations. *Math. Comp.* **87**, 2977–3021 (2018).
[3] T. Dreyfus; C. Hardouin; J. Roques, Hypertranscendence of solutions of Mahler equations. *J. Eur. Math. Soc.* **20**, 2209–2238 (2018).
[4] J. Roques, On the algebraic relations between Mahler functions. *Trans. Amer. Math. Soc.* **370**, 321–355 (2018).

Factoring linear recurrence operators

Mark van Hoeij[1] [hoeij@math.fsu.edu]

[1] Florida State University, Tallahassee, FL 32306

Several computer algebra systems have implementations for finding hypergeometric solutions of linear recurrence equations. This is equivalent to finding first order factors of linear recurrence operators. This talk will present several approaches to compute higher order factors of operators in $\mathbb{Q}(x)[\tau]$ where τ is the shift operator.

Keywords
Recurrence equations, recurrence operators, shift operator, factorization

A decision algorithm for strong rational general solutions of algebraic ordinary differential equations

Franz Winkler[1] [franz.winkler@risc.jku.at]

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

We consider first-order algebraic ordinary differential equations (AODEs) and study their rational general solutions. A rational general solution of a first-order AODE contains an arbitrary constant. In case the constant appears rationally, we call the solution strong. We present an algorithm for deciding the existence of a strong rational general solution of a first-order AODE, and in the positive case, compute such a solution. The problem of computing a rational general solution of first-order AODEs has not yet been solved in full generality. Our method is based on optimal parametrizations of algebraic curves over the field of rational functions.

Consider the first-order AODE,

$$F(x, y, y') = 0\ ,$$

where F is an irreducible polynomial in three variables over an algebraically closed field $\mathbb{K}$. Replacing y' by a new indeterminate z, we obtain an algebraic equation $F(x, y, z) = 0$. This algebraic equation defines a plane algebraic curve

$$\mathscr{C} := \{(a, b) \in \mathbb{A}^2(\overline{\mathbb{K}(x)}) \mid F(x, a, b) = 0\}$$

over the field $\overline{\mathbb{K}(x)}$ of algebraic functions. We call it the corresponding algebraic curve. A parametrization of $\mathscr{C}$ is a rational map

$$\mathscr{P} : \mathbb{A}^1(\overline{\mathbb{K}(x)}) \to \mathscr{C} \subset \mathbb{A}^2(\overline{\mathbb{K}(x)})\ ,$$

such that the image of $\mathscr{P}$ is dense in $\mathscr{C}$ with respect to the Zariski topology. If furthermore $\mathscr{P}$ is a birational equivalence, it is called a proper parametrization. A parametrization is represented as a pair of rational functions, say $\mathscr{P} = (p_1(t), p_2(t))$, with coefficients in $\overline{\mathbb{K}(x)}$. The field which extends $\mathbb{K}(x)$ by coefficients of $\mathscr{P}$ is called the field of coefficients of $\mathscr{P}$. In case the degree of the field of coefficients over $\mathbb{K}(x)$ is as small as possible, we call $\mathscr{P}$ an optimal parametrization. It is well known that the field of coefficients of an optimal parametrization has at most algebraic extension degree 2 over $\mathbb{K}(x)$.

A rational solution of the differential equation $F(x, y, y') = 0$ is a rational function $y(x) \in \mathbb{K}(x)$, such that $F(x, y(x), y'(x)) = 0$. According to Ritt [1] the radical differential ideal $\{F\}$ can be decomposed as

$$\{F\} = \underbrace{\left(\{F\} : \frac{\partial F}{\partial y'}\right)}_{\textit{general component}} \cap \underbrace{\left\{F, \frac{\partial F}{\partial y'}\right\}}_{\textit{singular component}}\ .$$

S is the separant of F, i.e., the derivative of F w.r.t. $y^{(n)}$). Ritt shows that the general component is a prime differential ideal; its generic zero is called a *general solution* of the AODE $F(x, y, y') = 0$. Such a general solution must contain a transcendental constant c. In [2, 3] we have presented a method for determining rational general solutions of first-order AODEs. This method is based on rational parametrization of surfaces. Whereas it can determine rational general solutions for almost all parametrizable first-order AODEs, it is not a decicion algorithm.

Here we are a little more modest, and we aim at determining so-called strong rational general solutions. A solution $y(x)$ of the AODE is called a *strong rational general solution*, if $y = y(x,c) \in \mathbb{K}(x,c) \setminus \mathbb{K}(x)$, where c is a transcendental constant over $\mathbb{K}(x)$. So a strong rational general solution is a proper rational function in x and c over $\mathbb{K}$.

The key fact with allows to decide the existence of strong rational general solutions, and in the positive case compute them, is the following:

Theorem *Let $F \in \mathbb{K}(x)[y,z]$ be an irreducible polynomial. If the algebraic curve in $\mathbb{A}^2(\overline{\mathbb{K}(x)})$ defined by $F = 0$ is a rational curve, then the coefficient field of its optimal parametrization is always $\mathbb{K}(x)$.*

A full description of this decision method can be found in [4].

Keywords
ordinary differential equation, algebraic curve, rational parametrization, rational general solution

References

[1] J.F. Ritt, *Differential Algebra.* Colloquium Publications, vol.33, Amer.Math.Society, 1950.
[2] L.X.C. Ngô, F. Winkler, Rational general solutions of first order non-autonomous parametrizable ODEs, *J. Symbolic Computation* **45**(12), 1426–1441 (2010).
[3] L.X.C. Ngô, F. Winkler, Rational general solutions of planar rational systems of autonomous ODEs, *J. Symbolic Computation* **46**(10), 1173–1186 (2011).
[4] N.T. Vo, G. Grasegger, F. Winkler, Deciding the existence of rational general solutions for first-order algebraic ODEs, *J. Symbolic Computation* **87**, 127–139 (2018).

S2 - Algebraic Geometry from an Algorithmic Point of View

On algebraic and geometric properties of almost revlex ideals

Cristina Bertone[1]***, Francesca Cioffi***[2] [cristina.bertone@unito.it]

[1] Dipartimento di Matematica “G. Peano”, Università di Torino
[2] Dipartimento di Matematica e Appl. “R. Caccioppoli”, Università di Napoli Federico II

Let $\Bbbk$ be an infinite field, and consider $R = \Bbbk[x_1, \dots, x_n]$ with the degrevlex term order on the variables $x_1 > \cdots > x_n$.

Definition. A monomial ideal $J \subset R$ is *almost reverse lexicographic* (*almost revlex* for short) if for every τ in the minimal monomial basis of J and for every term σ, if $\sigma > \tau$ then σ belongs to J.

Almost revlex Artinian ideals have a prominent role in Moreno-Socias' conjecture [6]:
The generic initial ideal (with respect to degrevlex term order) of a polynomial ideal $I \subset R$ generated by r generic forms is the almost reverse lexicographic ideal J such that the Hilbert function of R/J is the same as that of R/I.

Almost revlex ideals are also *strongly stable*, and this feature makes them very attracting in order to study the Hilbert scheme $\mathrm{Hilb}^{\mathbb{P}^n}_{p(z)}$, see for instance [4]. This Hilbert scheme parameterizes subschemes defined by saturated homogeneous ideals I in $\Bbbk[x_0, \dots, x_n]$ such that the quotient ring $\Bbbk[x_0, \dots, x_n]/I$ has Hilbert polyomial $p(z)$.

With these two motivations of interest in our mind, in [1] we investigate almost revlex ideals, in particular Artinian ones having the same Hilbert function as a complete intersection.

First, we investigate reduction numbers of almost revlex ideals (also non-Artinian ones). If J is a strongly stable ideal, its *s-th reduction number* r_s is $\min\{t \mid x_{n-s}^{t+1} \in J\}$ [5, Corollary 1.4]. We prove the positivity of the s-th derivative $\Delta^s H$ of the Hilbert function H of R/J at t, with $t \leq r_s$. As a consequence, we obtain a closed formula for the cardinality of the minimal monomial basis generating an almost revlex ideal.

Theorem. Let $J \subset R$ be an almost revlex ideal and B_J its minimal monomial basis, δ the Krull dimension and H the Hilbert function of R/J. Then,

$$|B_J| = \begin{cases} \sum_{s=0}^{n-1} \Delta^s H(r_{s+1}), & \text{if } \delta = 0 \\ \sum_{s=\delta}^{n-1} \Delta^s H(r_{s+1}) + \Delta^{\delta-1} H(r_\delta) - \Delta^{\delta-1} H(\varrho), & \text{if } \delta > 0 \end{cases} \tag{1}$$

where $\varrho = \min\{t : \Delta^{\delta-1} H(j) = \Delta^{\delta-1} H(j+1), \forall j \geq t\}$.

With a better comprehension of the meaning that reduction numbers of almost revlex ideals have with respect to the positivity of the derivatives of the Hilbert function, given the Hilbert function H of an Artinian complete intersection, we describe an explicit construction of the almost reverse lexicographic ideal $J \subset R$ such that the Hilbert function of R/J is H [1, Theorem 4.1].

In [7, Theorems 4 and 5, Corollary 6] K. Pardue gave a complete characterization of the Hilbert functions that admit almost reverse lexicographic ideals, and among them there are the Hilbert functions of complete intersections. Our method gives a new insight in the complete intersection case, since we proceed inductively on n using Hilbert functions of complete intersections at each step. The role of reduction numbers is crucial in the arguments we use.

If $J \subset R$ is an Artinian monomial ideal, we denote by $J' := J \cdot R[x_{n+1}]$ the saturated monomial ideal generated by J in the ring $R[x_{n+1}]$. The projective scheme $\mathrm{Proj}(R[x_{n+1}]/J')$ belongs to the Hilbert scheme Hilb^n_D, where D is the cardinality of the set of terms in R not belonging to J. Using marked schemes, (see for instance [2,3]), we investigate conditions ensuring that J' is a singular point of Hilb^n_D. First, we obtain the following result, which applies to the wider class of *stable* ideals.

Theorem. Let $J \subset R$ be an Artinian stable ideal. Let J' and Hilb^n_D as above. Furthermore, let $\mathcal{T}_{J'}$ be the Zariski tangent space to Hilb^n_D at its point $\mathrm{Proj}(R[x_{n+1}]/J')$. Then

$$|B_J| \cdot |\{\tau \in B_J : x_n \text{ divides } \tau\}| \le \dim \mathcal{T}_{J'} \le |B_J| \cdot D.$$

Since the Hilbert scheme Hilb^n_D always has a component of dimension $n \cdot D$ (the *principal component*) and the scheme corresponding to every strongly stable ideal lies on this component (see for instance [8]), we immediately have:

Corollary. Let $J \subset R$ be an Artinian stable Borel-fixed ideal. The scheme $\mathrm{Proj}(R[x_{n+1}]/J')$ is a singular point in Hilb^n_D if $|B_J| \cdot |\{\tau \in B_J : x_n \text{ divides } \tau\}| > n \cdot D$.

Finally, let H be the Hilbert function of a complete intersection defined by n forms of degrees $d_1 \le \cdots \le d_n$, let J be the Artinian almost revlex ideal with Hilbert function H and $J' = J \cdot R[x_{n+1}]$. We observe that in this setting the number $|\{\tau \in B_J : x_n \text{ divides } \tau\}|$ is exactly $H(r_1)$. In [1, Corollaries 6.6 and 6.7] we exhibit several cases, depending on n and the integers d_i's, ensuring that J' corresponds to a singular point in the Hilbert scheme Hilb^n_D. For instance: for every $n \ge 3$ and $2 \le d = d_1 = d_n$, J' corresponds to a singular point in the Hilbert scheme Hilb^n_D.

The arguments to prove this statement (and others) also involve the formula for the number of minimal monomial generators of J and the sufficient condition for the dimension of the Zariski tangent space to be higher than the dimension of the principal component of Hilb^n_D. Only few cases are handled by a direct computation of the dimension of the Zariski tangent space to Hilb^n_D at J' by [3, Corollary 1.9 and Remark 1.10].

Keywords
almost revlex ideals, reduction number, complete intersection, Hilbert scheme

References

[1] C. BERTONE, F. CIOFFI, On almost revlex ideals with Hilbert function of complete intersections, preprint, arXiv:1803.02330 [math.AC].
[2] C. BERTONE, F. CIOFFI, M. ROGGERO, Macaulay-like marked bases. *Journal of Algebra and its Applications* **16** (5) (2017).
[3] C. BERTONE, F. CIOFFI, M. ROGGERO, Smoothable Gorenstein Points Via Marked Schemes and Double-generic Initial Ideals. *Experimental Mathematics*, to appear, doi:10.1080/10586458.2019.1592034.
[4] R. HARTSHORNE, Connectedness of the Hilbert scheme. *Inst. Hautes Études Sci. Publ. Math.* **29**, 5–48 (1966).
[5] L. T. HOA AND N. V. TRUNG, Borel-fixed ideals and reduction number, *J. Algebra* (270) 1, 335–346 (2003).
[6] G. MORENO-SOCIAS, Degrevlex Groebner bases of generic complete intersections. *J. Pure Appl. Algebra* **180** (3), 263–283 (2003).
[7] K. PARDUE, Generic sequences of polynomials. *J. Algebra* **324** (4), 579–590 (2010).
[7] A. A. REEVES, The radius of the Hilbert scheme, *J. Algebraic Geom.* **4** (4), 639–657 (1995).

Bar Code and Janet-like division

Michela Ceria[1] [michela.ceria@unimi.it]

[1] Department of Computer Science, Università degli Studi di Milano

Bar Codes are combinatorial objects encoding many properties of monomial ideals [1, 2, 3, 4]. They can be used as tools to study, describe and build Janet-like division, a divisibility relation on terms, introduced in [12, 13] to efficiently compute Groebner bases.

Definition 1. A Bar Code B is a picture composed by segments, called *bars*, superimposed in horizontal rows, which satisfies conditions *a.*, *b.* below. Denoted by $\mathsf{B}_j^{(i)}$ the j-th bar (from left to right) of the i-th row (from top to bottom), $1 \le i \le n$, i.e. the *j-th i-bar*; $\mu(i)$ the number of bars of the i-th row; $l_1(\mathsf{B}_j^{(1)}) := 1$, $\forall j \in \{1,2,...,\mu(1)\}$ the $(1-)$*length* of the 1-bars and $l_i(\mathsf{B}_j^{(k)})$, $2 \le k \le n$, $1 \le i \le k-1$, $1 \le j \le \mu(k)$ the *i-length* of $\mathsf{B}_j^{(k)}$, i.e. the number of i-bars lying over $\mathsf{B}_j^{(k)}$:

a. $\forall i, j$, $1 \le i \le n-1$, $1 \le j \le \mu(i)$, $\exists! \overline{j} \in \{1,...,\mu(i+1)\}$ s.t. $\mathsf{B}_{\overline{j}}^{(i+1)}$ lies under $\mathsf{B}_j^{(i)}$

b. $\forall i_1, i_2 \in \{1,...,n\}$, $\sum_{j_1=1}^{\mu(i_1)} l_1(\mathsf{B}_{j_1}^{(i_1)}) = \sum_{j_2=1}^{\mu(i_2)} l_1(\mathsf{B}_{j_2}^{(i_2)})$; we will then say that *all the rows have the same length.* $\diamond$

We can associate a Bar Code to any finite set of terms and vice versa; we recall only the former procedure, being that used in this abstract. Let $\mathcal{T} := \{x^\gamma := x_1^{\gamma_1} \cdots x_n^{\gamma_n} \mid \gamma = (\gamma_1,...,\gamma_n) \in \mathbb{N}^n\}$ be the semigroup of terms in n variables and let $t \in \mathcal{T}$. For $1 \le i \le n$, we define $\pi^i(t) := x_i^{\gamma_i} \cdots x_n^{\gamma_n} \in \mathcal{T}$. Given $M \subset \mathcal{T}$, with $|M| = m < \infty$, we order its elements increasingly w.r.t. Lex, getting the list $\overline{M}$. Applying $\pi^i(t)$ to each t in $\overline{M}$, we get a new list $\overline{M}^{[i]}$, for $1 < i \le n$. Then we construct the matrix $\mathcal{M}$ whose i-th row is $\overline{M}^{[i]}$, $i = 1,...,n$. Underlining with a segment all the repeated terms in each row of $\mathcal{M}$ and deleting the terms, except from those in the first row, we get the desired Bar Code.

We recall now the definitions concerning Janet and Janet-like divisions, in order to introduce our main results. Janet division dates back to the 1920 paper [15] and it is defined, for each set of terms $U \subset \mathcal{T}$, as a divisibility relation on terms. In particular, each $t \in U$ is equipped with a set $M_J(t,U)$ of multiplicative variables, according to the following definition.

Definition 2. Let $U \subset \mathcal{T}$ be a set of terms A variable x_j is called *multiplicative* for t with respect to U if there is no term in U of the form $t' = x_1^{\beta_1} \cdots x_j^{\beta_j} x_{j+1}^{\alpha_{j+1}} \cdots x_n^{\alpha_n}$ with $\beta_j > \alpha_j$. We denote by $M_J(t,U)$ the set of multiplicative variables for t with respect to U, whereas the variables that are not multiplicative for t w.r.t. U are called *non-multiplicative* and we denote by $NM_J(t,U)$ their set. $\diamond$

The divisibility relation is defined as follows: for each $u \in \mathcal{T}$, we say that a term $t \in U$ Janet-divides u if $u = tv$ and each $x_j \mid v$, $j \in \{1,...,n\}$, belongs to $M_J(t,U)$. In this case, t is a Janet-divisor of u and u a Janet-multiple of t. The *cone* of t with respect to U is the set $C_J(t,U) := \{t x_1^{\lambda_1} \cdots x_n^{\lambda_n} \mid \text{where } \lambda_j \neq 0 \text{ only if } x_j \in M_J(t,U)\}$. A set $U \subset \mathcal{T}$ is *complete* if $\top(U) = \bigcup_{t \in U} C_J(t,U)$. Janet division is employed to construct a special kind of Groebner basis for a polynomial ideal $I = (G)$ called *Janet basis*. Roughly speaking, the complete set U is the set of all leading terms for the generators and any term $u \in \mathcal{T}$ is reduced by means of the polynomial $f \in G$ such that its leading term is the Janet-divisor of u.

A generalization of Janet division and Janet bases is given in [10, 11, 14], by defining involutive divisions and involutive bases. Janet-like division and Janet-like bases are introduced in [12,13] with the aim to decrease the number of elements in the basis.

Definition 3. Let $U \subset \mathcal{T}$ be a finite set of terms; for each $u \in U$, $1 \leq i \leq n$ consider $h_i(u,U) = \max\{\deg_i(v) : v \in U, \deg_j(v) = \deg_j(u), i+1 \leq j \leq n\} - \deg_i(u) \in \mathbb{N}$. If $h_i(u,U) > 0$, define $k_i := \min\{\deg_i(v) - \deg_i(u) : \deg_j(v) = \deg_j(u), i+1 \leq j \leq n, \deg_i(v) > \deg_i(u)\}$; then $x_i^{k_i}$ is called *non-multipicative power* of $u \in U$. We denote by $NMP(u,U)$ the set of nonmultiplicative powers for $u \in U$. $\diamond$

Definition 4. Let $U \subset \mathcal{T}$ be a finite set of terms and $u \in U$; the elements in the monoid ideal $NM(u,U) = \{v \in \mathcal{T} \mid \exists w \in NMP(u,U) : w \mid v\}$ are called Janet-like *nonmultipliers* for u, whereas the elements in $M(u,U) = \mathcal{T} \setminus NM(u,U)$ are called Janet-like *multipliers* for u. A term $u \in U$ is a *Janet-like divisor* of $w \in \mathcal{T}$ if $w = uv$ with $v \in M(u,U)$. $\diamond$

We remark that, though Janet-like division preserves many properties of Janet division, it is *not an involutive division.* A Bar Code can be used as a tool for studying Janet and Janet-like division. Indeed a Bar Code can help to assign to each element t of a finite $U \subset \mathcal{T}$ its multiplicative variables, according to Janet's definition. Let $U \subset \mathcal{T}$ be a finite set of terms and suppose $x_1 < x_2 < \ldots < x_n$; we can associate a Bar Code B to it. Then $\forall 1 \leq i \leq n$, place a star symbol $*$ on the right of $\mathsf{B}^{(i)}_{\mu(i)}$. Moreover, let $\mathsf{B}^{(i)}_j$ and $\mathsf{B}^{(i)}_{j+1}$ $\forall 1 \leq i \leq n-1$, $\forall 1 \leq j \leq \mu(i)-1$ be two consecutive bars not lying over the same $(i+1)$-bar; place a star symbol $*$ between them.

Theorem 5. [5] Let $U \subseteq \mathcal{T}$ be a finite set of terms and B_U its Bar Code. For each $t \in U$, x_i, $1 \leq i \leq n$, is multiplicative for t if and only if the i-bar under t in B_U is followed by a star. $\diamond$

Every nonmultiplicative power is nothing else then the power of a Janet-nonmultiplicative variable [13] and this reflects on the Bar Code associated to U.

Proposition 6. Let $U \subseteq \mathcal{T}$ be a finite set of terms and B_U its Bar Code. Let $t \in U$, $x_i \in NM_J(t,U)$, $\mathsf{B}^{(i)}_l$ the i-bar under t and t' any term over $\mathsf{B}^{(i)}_{l+1}$. Then $k_i = \deg_i(t') - \deg_i(t)$.$\diamond$

A set $U \subset \mathcal{T}$ is called *complete* w.r.t. Janet-like division if $C(U) = C_J(U)$ for the sets $C_J(U) := \{uv : u \in U, v \in M(u,U)\}$ and $C(U) := \{uv : u \in U, v \in \mathcal{T}\}$. This is equivalent to say that $\forall u \in U$, $\forall p \in NMP(u,U)$, $\exists v \in U : v \mid up$ w.r.t. Janet-like division.

Theorem 7. Let $U \subset \mathcal{T}$ be a finite set of terms, B its Bar Code, $t \in U$, $p = x_i^{k_i} \in NMP(t,U)$ and $\mathsf{B}^{(i)}_j$ the i-bar under t. Let $s \in U$; $s \mid tp$ w.r.t. Janet-like division if and only if $s \mid pt$, s lies over $\mathsf{B}^{(i)}_{j+1}$ and $\forall j'$ such that $x_{j'} \mid \frac{pt}{s}$ either there is a star after the j'-bar under s or the nonmultiplicative power w.r.t. $x_{j'}$ has degree greater than $deg_{j'}(\frac{pt}{s})$. $\diamond$

We conclude sketching how to compute the Janet-like reduced basis for a zerodimensional radical ideal $I := I(\mathbf{X})$ of the polynomial ring $\mathbf{k}[x_1, \ldots, x_n]$ in n variables over a field $\mathbf{k}$, given its (finite) variety $\mathbf{X} = \{P_1, \ldots, P_N\}$, *avoiding the classical Buchberger reduction*, which is known to be a computationally heavy task. The paper [16] proposes four methods to compute the normal form of a polynomial w.r.t. I, without passing through Groebner bases.

Proposition 8. [16] Let $\mathbf{X} = \{P_1, ..., P_N\}$ be a finite set of points, $I := I(\mathbf{X}) \triangleleft \mathbf{k}[x_1, ..., x_n]$ its 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 $\mathrm{Nf}(f, \mathsf{N})$ is the normal form of f w.r.t. N and $\mathsf{N}[[\mathbf{X}]]$ is the matrix whose rows are the evaluations of the elements of N at all points. $\diamond$

If we want to compute a reduced Janet-like basis for I given $\mathbf{X}$, we only need the points in $\mathbf{X}$, a basis N for the quotient algebra $A := \mathbf{k}[x_1, ..., x_n]/I$ and a complete set U of terms w.r.t. Janet-like division, which generates the semigroup ideal of leading terms $\mathsf{T}(I)$, so that the basis is the set $B = \{\mathrm{Nf}(t, \mathsf{N}) : t \in U\}$. A very simple basis for A is the lexicographical Groebner escalier $\mathsf{N}(\mathbf{X})$ of I and it can be computed in a purely combinatorial way, without using Groebner bases [4, 8, 9, 16]. Once one has the escalier, it is a trivial task to find a generating set U for $\mathsf{T}(I)$. Finally, one can construct the Bar Code associated to U and use Theorem 7 to update it dinamically by adding those terms of the form tv, $t \in U$, $v \in NMP(t, U)$ such that it has no Janet-like divisors in U. This way, we can get a completion of U and a simple application of Proposition 8 to the elements of the completion gives the desired basis, following the approach of [6, 7].

References

[1] Michela Ceria. *Applications of Bar Code to involutive divisions and a greedy algorithm for complete sets.* In preparation.

[2] Michela Ceria. *Bar code: a visual representation for finite sets of terms and its applications.* Submitted (2018).

[3] Michela Ceria. *Bar code for monomial ideals* Journal of Symbolic Computation `DOI:https://doi.org/10.1016/j.jsc.2018.06.012` Volume 91,2019, 30–56.

[4] Michela Ceria and Teo Mora. *Combinatorics of ideals of points: a Cerlienco- Mureddu-like approach for an iterative lex game.* In preparation.

[5] Michela Ceria, *Bar Code vs Janet tree.* Submitted (2019).

[6] Michela Ceria, Teo Mora, and Andrea Visconti. *Efficient computation of squarefree separator polynomials.*. Submitted (2018).

[7] Michela Ceria, Teo Mora, and Andrea Visconti. *Efficient computation of squarefree separator polynomials (extended abstract).* In International Congress on Mathematical Software. Springer, 98–104 (2018).

[8] Luigi Cerlienco and Marina Mureddu. *Algoritmi combinatori per l'interpolazione polinomiale in dimensione* ≥ 2. Séminaire Lotharingien de Combinatoire 24 p. 39–76 (1990).

[9] Bálint Felszeghy, Balázs Ráth, and Lajos Rónyai. *The lex game and some applications.* Journal of Symbolic Computation 41, 6 (2006), 663–681.

[10] Vladimir P Gerdt and Yuri A Blinkov. *Involutive bases of Polynomial Ideals.* Math. Comp. Sim. 45 (1998), 543–560.

[11] Vladimir P Gerdt and Yuri A Blinkov. *Minimal involutive bases.* Math. Comp. Sim. 45 (1998), 519–541.

[12] Vladimir P Gerdt and Yuri A Blinkov. *Janet-like Gröbner bases.* In International Workshop on Computer Algebra in Scientific Computing. Springer, 184–195, 2005.
[13] Vladimir P Gerdt and Yuri A Blinkov. *Janet-like monomial division.* In International Workshop on Computer Algebra in Scientific Computing. Springer, 174–183, 2005.
[14] Vladimir P Gerdt and Yuri A Blinkov. *Involutive Division Generated by an Antigraded Monomial Ordering.* L. N. Comp. Sci 6885 (2011), 158–174.
[15] Maurice Janet. *Sur les systèmes d'équations aux dérivées partelles.* J. Math. Pure et Appl. 3 (1920), 55–151.
[16] Samuel Lundqvist. *Vector space bases associated to vanishing ideals of points.* Journal of Pure and Applied Algebra 214, 4 (2010), 309–321.

Some new elementary components of the Hilbert scheme of points

Mark Huibregtse[1] [mhuibreg@skidmore.edu]

[1] Department of Mathematics and Statistics, Skidmore College, Saratoga Springs, NY USA

Let K be an algebraically closed field of characteristic 0, and

$$\mathbb{A}_K^n = \operatorname{Spec}(K[x_1, \ldots, x_n] = K[\mathbf{x}])$$

the affine space of dimension n. The Hilbert scheme of μ points of $\mathbb{A}_K^n$, denoted $H^{\mu}_{\mathbb{A}_K^n} = H$, parametrizes the 0-dimensional closed subschemes of length μ of $\mathbb{A}_K^n$, or, equivalently, the ideals $I \subseteq K[\mathbf{x}]$ such that $\dim_K(K[\mathbf{x}]/I) = \mu$ (we say such ideals have **colength** μ). We denote the point of H corresponding to the ideal I by $[I]$.

The **principal component** of H is the closure of the locus of points $[I]$ such that the corresponding subscheme $\operatorname{Spec}(K[\mathbf{x}]/I)$ is supported at μ distinct points of $\mathbb{A}_K^n$. It is known that H is irreducible (and so equal to its principal component) when $n < 3$, but reducible for $n \geq 3$ and $\mu >> 0$; the latter was shown by Iarrobino in [2]. An **elementary component** of H is an irreducible component E such that for every point $[I] \in E$, the support of the corresponding subscheme is a single point of $\mathbb{A}_K^n$. Since every irreducible component of H is generically a product of elementary components, the elementary components can be viewed as "building blocks" of H.

The first non-trivial examples of elementary components were given by Iarrobino and Emsalem in [3]. Our examples are generalizations of their well-known example with Hilbert function $(1,4,3)$: The ideal $I \subseteq K[x_1, \ldots, x_4]$ is generated by seven quadratic forms

$$g_j = m_j - N_j,\ 1 \leq j \leq 7,$$

where m_j is the j-th monomial in the list of "leading" monomials

$$\mathrm{LM} = x_1^2, x_1x_2, x_1x_3, x_1x_4, x_2^2, x_2x_3, x_2x_4,$$

and

$$N_j = \sum_{i=0}^{2} (c_{ij} \cdot x_3^i x_4^{2-i})$$

is a K-linear combination of the "trailing" monomials $\mathrm{TM} = \{x_3^2, x_3x_4, x_4^2\}$ of degree 2 in the "back variables" x_3, x_4. When the coefficients c_{ij} are sufficiently general, one can show that all the monomials of degree 3 belong to I; consequently, I has finite colength with the origin as zero-set, and one sees easily that the order ideal

$$\mathcal{O} = \{1, x_1, x_2, x_3, x_4, x_3^2, x_3x_4, x_4^2\}$$

is a K-basis of the quotient $K[\mathbf{x}]/I$. (Recall that an **order ideal** is a set of monomials $\mathcal{O}$ such that whenever m_1, m_2 are monomials such that $m_1 \in \mathcal{O}$ and $m_2 | m_1$, it follows that $m_2 \in \mathcal{O}$.) The point $[I]$ can be moved to nearby points $[I']$ parameterizing subschemes supported at one point in two ways: tweaking the 21 coefficients c_{ij}, and translating in the four independent directions in $\mathbb{A}^4_K$. One finds by computation that the tangent space dimension at $[I]$ is 25, which implies that $[I]$ is a smooth point on an elementary component of dimension 25. Note that the principal component has dimension $n\mu = 4 \cdot 8 = 32$.

In [Hui], we presented some new examples of elementary components in which the leading and trailing monomials have different degrees. In our simplest example of Hilbert function $(1,5,3,4)$, the leading monomials are the 12 monomials of degree 2 in $K[x_1,\dots,x_5]$ that involve at least one of the "front variables" x_1, x_2, x_3:

$$\mathrm{LM} = \left\{ \begin{array}{c} x_1^2,\ x_1x_2,\ x_1x_3,\ x_1x_4,\ x_1x_5,\ x_2^2,\ x_2x_3, \\ x_2x_4,\ x_2x_5, x_3^2,\ x_3x_4,\ x_3x_5 \end{array} \right\},$$

and the trailing monomials are the four monomials of degree 3 in the "back variables" x_4, x_5:

$$\mathrm{TM} = \{x_4^3,\ x_4^2x_5,\ x_4x_5^2,\ x_5^3\}.$$

The ideal I is again generated by polynomials

$$g_j = m_j - N_j,\ 1 \le j \le 12,$$

where m_j is the j-th leading monomial and N_j is a K-linear combination of the trailing monomials.

If the g_j are sufficiently general, it can be shown that every monomial of degree 4 is in I, and that the quotient $K[\mathbf{x}]/I$ has for K-basis the order ideal

$$\mathcal{O} = \left\{1,\ x_1,\ x_2,\ x_3,\ x_4,\ x_5,\ x_4^2,\ x_4x_5,\ x_5^2,\ x_4^3,\ x_4^2x_5,\ x_4x_5^2,\ x_5^3\right\},$$

so $[I] \in H^{13}_{\mathbb{A}^5_K}$.

There are three ways to move $[I]$ while keeping the support a single point: the 48 coefficients can be tweaked, the ideal can be translated in 5 independent directions, and it can be pulled back via automorphisms of $\mathbb{A}^5_K$ of the form $x_\alpha \to x_\alpha + c_{\alpha,\beta} \cdot x_\beta$, $x_\beta \to x_\beta$, where $1 \le \alpha \le 3$, $4 \le \beta \le 5$, $c_{\alpha,\beta} \in K$. Therefore, $[I]$ lies on a locus of dimension at least $48+5+3\cdot 2 = 59$ consisting of points $[I']$ such that the ideal I' is supported at one point. On the other hand, one computes that the dimension of the tangent space at $[I]$ is 59. From this it follows that $[I]$ is a smooth point on an elementary component of $H^{13}_{\mathbb{A}^5_K}$ of dimension 59. The dimension of the principal component in this case is $5 \cdot 13 = 65$.

Our newest examples are similar to those presented in [1], but involve an additional way to move the ideal I. Here is our simplest example: we have five variables $x_1,\dots,x_5$. The front variables are x_1, x_2, the "middle variable" is x_3, and the "back variables" are x_4, x_5. The leading and trailing monomial sets are

$$\begin{array}{rcl} \mathrm{LM} & = & \{x_1^2, x_1x_2, x_1x_3, x_1x_4, x_1x_5, x_2^2, x_2x_3, x_2x_4, x_2x_5, x_3^2\} \\ \mathrm{TM} & = & \{x_3x_4^2, x_3x_4x_5, x_3x_5^2, x_4^3, x_4^2x_5, x_4x_5^2, x_5^3\}. \end{array}$$

For sufficiently general polynomials of the form $g_j = m_j - N_j$, as before, the ideal $I = (\{g_j\})$ will contain all the monomials of degree 4 (and therefore have the origin as support), and the quotient $K[\mathbf{x}]/I$ will be K-free with basis

$$\begin{array}{rcl} \mathcal{O} & = & \{1, x_1, x_2, x_3, x_4, x_5, x_3x_4, x_3x_5, x_4^2, x_4x_5, x_5^2, \\ & & x_3x_4^2, x_3x_4x_5, x_3x_5^2, x_4^3, x_4^2x_5, x_4x_5^2, x_5^3\}, \end{array}$$

so the Hilbert function of I is $(1,5,5,7)$ and $[I] \in H^{18}_{\mathbb{A}^5_K}$. We divide the monomials in x_3, x_4, x_5 into "segments" based on their x_3-degree; in this case, the leading monomials end with the segment $\{x_3^2\}$ and the degree-2 monomials in $\mathcal{O}$ begin with the segment $\{x_3x_4, x_3x_5\}$. We can again move $[I]$ by tweaking the $7 \cdot 10 = 70$ coefficients in the N_j, translating in five independent directions, and pulling back the ideal via certain automorphisms (there are 8 in this case), giving $70 + 5 + 8 = 83$ independent ways to move $[I]$ to nearby points $[I']$ representing irreducible subschemes. By computation, we find that the tangent space dimension at $[I]$ is 86. However, there are three more independent ways to move $[I]$, which we call "modifications," obtained by adding a term (one of $\{tx_4^2, tx_4x_5, tx_5^2\}$ to $g_{10} = x_3^2 - N_{10}$, and then adding two polynomials to the list of ideal generators to ensure that the modified ideal remains in $H^{18}_{\mathbb{A}^5_K}$ for all values of the parameter t. For instance, if we add the term tx_4^2 to g_{10}, then we add the generators $x_3^2x_4 + tx_4^3$ and $x_3^2x_5 + tx_4^2x_5$. We obtain in this way a one-parameter family of points $[I(t)]$ in $H^{18}_{\mathbb{A}^5_K}$ with $[I(0)] = I$, which yields a tangent direction at $[I]$ that is independent of the 83 already found. Hence, $[I]$ is a smooth point on an elementary component of dimension 86. Note that the principal component in this case has dimension $5 \cdot 18 = 90$. The presentation will describe in further detail the definition and algorithmic construction of the modifications, and exhibit additional new examples of elementary components.

Contrary to my initial intuition, it appears that the analogous example with Hilbert function $(1,5,4,5)$ does not yield an elementary component, whereas the "surrounding" examples of Hilbert functions $(1,5,5,7)$ and $(1,5,3,4)$ both do. This is connected to recent work of Jelisiejew [4], which describes a different approach to finding elementary components.

Keywords
Hilbert scheme of points , elementary component

References

[1] M. BREGTSE, Some elementary components of the Hilbert scheme of points. *Rocky Mt. J. Math.* **47** (4), 1169–1225 (2017).

[2] A. IARROBINO, Reducibility of the families of 0-dimensional schemes on a variety. *Invent. Math.* **15**, 72–77 (1972).
[3] A. IARROBINO; J. EMSALEM, Some Zero-Dimensional Generic Singularities: Finite Algebras Having Small Tangent Space. *Compositio Mathematica* **36**, 145–188 (1978).
[4] J. JELISIEJEW, Elementary components of Hilbert schemes of points.
Available at arXiv:1710.06124[Math.AG].

Unrestricted dynamic Gröbner Basis algorithms

Gabriel Mattos Langeloh[1] [gmlangeloh@inf.ufrgs.br]

[1] Instituto de Informática, Departamento de Informática Teórica, Universidade Federal do Rio Grande do Sul, Porto Alegre, Brazil

Gröbner Bases are a useful tool to compute with ideals of polynomial rings, with applications in polynomial system solving, cryptography and error-correcting codes, for example. It makes sense to try to choose monomial orderings leading to *small* Gröbner Bases in number of polynomials, monomials and degrees of their elements as this may, in some cases, lead to shorter computation times or lower memory usage. This problem was previously studied in [1, 2, 4, 5, 6, 8].

Choosing orderings leading to small Gröbner Bases *a priori* is hard, as the size of the output basis is often hard to predict. For this reason, [1, 4] introduced *dynamic Buchberger algorithms*, variations of Buchberger's traditional algorithm that allow the monomial ordering to change during the computation, usually leading to smaller output bases. Dynamic algorithms evaluate monomial orderings with heuristics, which are often based on the Hilbert function of an initial ideal, every time a new polynomial is added to the basis.

Most previously proposed dynamic algorithms are *restricted*, which means that after choosing a leading monomial for a polynomial in the basis, this choice cannot be undone. All restricted algorithms are based on linear programming, so choosing new monomial orderings has a relatively high overhead. On the other hand, *unrestricted* algorithms allow previous leading monomials to change. Until now, the only unrestricted algorithm had been introduced in [4]. This algorithm evaluates the entire space of monomial orderings whenever a new polynomial is added to the partial Gröbner Basis, and is very slow even for ideals of moderate size. The main goal of this work is to introduce alternative unrestricted dynamic Buchberger algorithms exploring fewer orderings, but hopefully still leading to small Gröbner Bases.

We experimented with four new strategies to explore the space of monomial orderings in an unrestricted manner. The *Random* algorithm generates a number of random orderings before each reduction, then picks the best one heuristically. The *Perturb* algorithm applies small perturbations to orderings, keeping the one with the best heuristic value found. Similarly, the *Simplex* algorithm obtains orderings that are "close" to the current one at each reduction, but instead of using perturbations, it uses linear programming and sensitivity analysis. Finally, the *Regrets* algorithm uses the same rules as the restricted algorithm of [1], but additionally chooses a polynomial in the basis and allows its leading monomial to change. In any unrestricted dynamic algorithm, it is necessary to rebuild the queue of S-polynomials whenever leading monomials of previous polynomials in the basis change. This can be done, for example, by successive application of the Gebauer-Möller criterion [3].

We implemented the four algorithms above based on Caboara and Perry's Sage implementation of their restricted algorithms [2]. In addition to our four algorithms, we experimented with the classical *Static* Buchberger algorithm, the original restricted algorithm *Caboara* [1] and the improved restricted algorithm *CP* [2], with their implementations unchanged from [2]. Also, we implemented the original unrestricted algorithm *GS* [4] and the algorithm *GS-then-CP*, that consists of a small number of iterations of the GS algorithm, followed by the CP algorithm. It roughly corresponds to applying the CP algorithm to a good initial ordering.

The implementations all share the core functionality of Buchberger's algorithm, such as reductions and S-polynomial queue updates using the Gebauer-Möller update strategy. We ran all algorithms on 141 benchmark input ideals with 2 to 8 variables over finite fields, with timeouts of 30 minutes. The implementations are meant as proofs of concept, and little effort was made to optimize them. Full results are presented in [7] and the code is available from `https://github.com/gmlangeloh/dynamic-experiments`.

	static	caboara	cp	gs	gs-then-cp	perturb	random	regrets	simplex	inst. solved
static		1.40	1.31	1.57	1.48	1.30	1.36	1.23	1.28	127
caboara	1.33		0.93	1.20	1.05	0.92	0.97	0.95	0.90	104
cp	1.29	0.96		1.27	1.14	1.02	1.06	1.00	0.98	112
gs	0.86	0.86	0.83		0.94	0.88	0.93	0.82	0.83	58
gs-then-cp	1.20	0.88	0.92	1.07		0.89	0.93	0.88	0.86	110
perturb	0.95	0.73	0.76	1.07	0.82		1.04	0.96	0.96	103
random	1.00	0.77	0.80	1.02	0.90	1.04		0.92	0.92	104
regrets	1.21	1.01	1.04	1.24	1.15	1.30	1.27		1.02	91
simplex	0.95	0.75	0.77	1.06	0.86	1.01	0.98	0.78		88

Table 1: Pairwise comparison between dynamic algorithms with respect to number of polynomials in basis (above the main diagonal) and maximum degree of polynomial in basis (below the main diagonal). Each value a_{ij} corresponds to the geometric mean of the ratios of the size of the output Gröbner Basis of algorithm in row i by that in column j, if $i < j$, or the geometric mean of ratios of the maximum degree in the output basis, otherwise. For values larger than 1, j is preferable to i. Pairwise comparisons are taken over instances in which neither algorithm timed out. The column inst. solved shows how many instances were solved by each algorithm within the time limit.

Table 1 shows our results for the size of the bases, in number of polynomials, and the maximum degrees of the polynomials in the output bases. We observe that all dynamic algorithms lead to bases with fewer polynomials than the classical static Buchberger algorithm, and that the original unrestricted GS algorithm returns the smallest bases in both number of polynomials and degree, but solves very few instances. It is worth mentioning that, although very simple, the Random and Perturb algorithms lead to slightly smaller bases in average than the CP algorithm, and slightly larger than Caboara's algorithm. In fact, both the Random and Perturb algorithms performed remarkably well, in spite of their simplicity. With appropriate adjustments, they could lead to dynamic algorithms with very small overhead, as they do not depend on linear programming like the restricted algorithms. We also remark that GS-then-CP leads to significantly smaller bases than CP, implying that starting the execution from a good initial ordering leads to better results. This comes, however, with the cost of higher running time.

Additionally, the restricted algorithms lead to polynomials of much higher degree when compared to the static algorithm, while the unrestricted algorithms, with the exception of Regrets, do not. We point out that the restricted and unrestricted algorithms perform well over different instances, and so their behavior may complement each other. Although this cannot be seen in the table, unfortunately the dynamic algorithms run for longer on average than the Static algorithm, although in many cases they perform fewer S-reductions, meaning that with further optimization they could be able to outperform the Static algorithm more often.

Future work will focus on adjusting parameters for the Random and Perturb algorithms, such as the number of samples used, and developing new unrestricted algorithms that use both as components. The space of monomial orderings should then be explored more effectively, as the Random algorithm uses no locality information on the monomial orderings, and Perturb has no mechanism to avoid being stuck at local optima.

It would also be interesting to perform similar experiments on benchmarks with more variables to obtain information on which algorithms scale better. This would require to implement the core of Buchberger's algorithm more efficiently. Another profitable research path is to study the behavior of the dynamic algorithms over other Gröbner Basis computation algorithms, such as F4 and F5.

Keywords
Gröbner Bases, Dynamic Algorithm, Monomial Ordering

References
[1] M. Caboara, A Dynamic Algorithm for Gröbner Basis Computation. In *Proc. of the 1993 International Symposium on Symbolic and Algebraic Comp.*, M. Bronstein (ed.), 275–283. ACM, 1993.
[2] M. Caboara; J. Perry, Reducing the size and number of linear programs in a dynamic Gröbner Basis algorithm. *Applicable Algebra in Engineering, Communications and Computing* **25**(1-2), 99–117 (2014).
[3] R. Gebauer; H. Möller, On an installation of Buchberger's algorithm. *J. Symb. Comp.* **6**(2-3), 275–286 (1988).
[4] P. Gritzmann; B. Sturmfels, Minkowski Addition of Polytopes: Computational Complexity and Application to Gröbner Bases. *SIAM J. Disc. Math.* **6**(2), 246–269 (1993).

[5] O. GOLUBITSKY, Converging term order sequences and the dynamic Buchberger algorithm. *Preprint*. 2006.
[6] A. HASHEMI; D. TALAASHRAFI, A Note on Dynamic Gröbner Bases Computation. In *Computer Algebra in Scientific Computing*, V. P. Gerdt, W. Koepf, W. M. Seiler, E. V. Vorozhtsov (eds.), 276–288. Springer, 2016.
[7] G. M. LANGELOH, Unrestricted dynamic Gröbner Basis algorithms. *Master's thesis.* Available at `https://lume.ufrgs.br/handle/10183/194287`.
[8] J. PERRY, Exploring the Dynamic Buchberger Algorithm. In *Proc. of the 2017 International Symposium on Symbolic and Algebraic Comp.*, M. Burr (ed.), 365–372. ACM, 2017.

New heuristics and extensions of the Dixon resultant for solving polynomial systems

Robert H. Lewis[1] [rlewis@fordham.edu]

[1] Mathematics Department, Fordham University, New York NY, USA

In this work “solve a system of polynomials" means to take a collection of multivariate polynomials, set each to 0, and search for the common roots. We have a ground ring K, variables $x_1, x_2, \ldots, x_n$, and parameters $a_1, a_2, \ldots, a_m$, so we are working over $K[a_1, \ldots, a_m, x_1, x_2, \ldots, x_n]$. K is primarily **Z**,**Q** or **Z/p** for p “large", $40000 - 2^{31}$. We are not interested in $K =$ **Z/2** or cryptology. We are not interested in purely numerical solution. We want an exact symbolic solution. We eliminate all but one of the variables, leaving one polynomial in one variable and the parameters – the *resultant* [1]. If desired, numerical values for the parameters can then be substituted, and the variable obtained numerically.

Classically, we have n equations in n variables. The system is neither over- nor under-determined. Always, $n \geq 2$; usually $3 \leq n \leq 15$. There are always parameters. Often there are as many parameters as variables.

The Bezout-Dixon method produces a matrix, which we denote M, whose determinant, $Det[M]$ is a multiple of the resultant. Dixon-EDF [5] is a way to compute the resultant without finding the entire determinant. Often the determinant is too large to compute, but has many factors, and so the resultant is much smaller than the determinant. We detect these polynomial factors “early," hence EDF = Early Detection of Factors. The output of the algorithm is a list of polynomials whose product is the determinant. Interesting problems tend to have many factors. On many real problems from interesting applications, EDF does very well [2], [3], [4].

In this work we present four new significant acceleration techniques and extensions to EDF.

Ordering of variables. We present a heuristic for the “weight" of a variable within the polynomial system. We use examples to show that the variables should be given precedence using this order, with the heaviest having the highest precedence. This can produce a smaller M with fewer and smaller entries.

Decomposing into blocks. It has long been noted that $Det[M]$ is often of the form qr^k, where q is spurious (of no interest) and r is the resultant. The exponent k is often in the range $2-6$. This suggests that matrix M could be decomposed into k blocks. We present a very fast way to produce this decomposition, if present, and show that huge speed-ups are possible.

Leaving M as a 2×2 matrix. Dixon-EDF row normalizes the matrix M in a special way. When finished, M is the identity matrix. However, there are large difficult problems with many parameters where at the 2×2 step, each of the four polynomials is so large that multiplying them is infeasible. Simply leaving M in that state can be a perfectly acceptable solution.

Dealing with more equations than variables. If there are more equations than variables, the Dixon resultant cannot be used even if the solution set is zero-dimensional. As a simple example, one may have a system of four linear equations in three variables that has a unique solution due to a nontrivial linear relationship between the equations. For a multivariate polynomial system, we present a method that can be very effective in converting the system into one that Dixon can solve.

Each new method will be illustrated with examples showing its great effectiveness.

Keywords
polynomial system, Dixon resultant, EDF, block decomposition

References

[1] D. Cox; J. Little; D. O'Shea, *Using Algebraic Geometry*. Graduate Texts in Mathematics 185, New York, 1998.

[2] R. Lewis; S. Bridgett, Conic tangency equations arising from Apollonius problems in biochemistry. *Mathematics and Computers in Simulation* **61**(2), 101–114 (2003).

[3] R. Lewis; E. Coutsias, Flexibility of Bricard's Linkages and Other Structures via Resultants and Computer Algebra *Mathematics and Computers in Simulation* **125**, 152–167 (2016).

[4] R. Lewis; P. Stiller, Solving the Recognition Problem for Six Lines Using the Dixon Resultant *Mathematics and Computers in Simulation* **49**, 203–219 (1999).

[5] R. Lewis, Dixon-EDF: The Premier Method for Solution of Parametric Polynomial. In *Springer Proceedings in Mathematics & Statistics*, I. Kotsireas, E. Martinez-Moro (eds.), 237–256. New York, 2017.

Weak Involutive bases over effective rings

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

[1] Department of Computer Science, University of Milan, Italy
[2] Department of Mathematics, University of Genoa, Italy

As remarked in 1992 by Schwartz [21], in 1920 after a cohoperation with Hilbert, Janet [11] introduced, under the name of complete/involutive bases both the notion of Gröbner bases and a computational algorithm which essentially anticipated Buchberger's [1,2] Algorithm† (apparently in the strongest formulation given by Moller's Lifting Theorem [14]). The recent extension of Buchberger Theory and Algorithm on each $\mathscr{R}$-module $\mathscr{A}$ [15, IV.50], [17, 5], where both $\mathscr{R}$ and $\mathscr{A}$ are assumed to be effectively given through their Zacharias representation [16] suggested us to investigate how far Janet's approach can be extended to more exotic settings. Clearly the combinatorial aspects of Janet completion necessarily require at least that, using the terminology of [15, IV.50], the associated graded ring $\mathscr{G}$ of $\mathscr{A}$ is an Ore-like extension [13, 6]; an interesting class of such rings, much wider than solvable polynomial rings [12] on which Seiler [22] applied Janet approach, has been recently proposed [18]: $\mathscr{A} = \mathscr{R}\langle X_1,\dots,X_n,Y_1,\dots,Y_m\rangle/\mathscr{I}, \mathscr{I} = \mathbb{I}(G)$ with

$$G = \{X_jX_i - a_{ij}X_iX_j - d_{ij} : 1 \le i < j \le n\} \cup \\ \cup \{Y_lX_j - b_{jl}v_{jl}X_jY_l - e_{jl} : 1 \le j \le n, 1 \le l \le m\} \cup \\ \cup \{Y_kY_l - c_{lk}Y_lY_k - f_{lk} : 1 \le l < k \le m\}$$

a Gröbner basis of $\mathscr{I}$ with respect to the lexicographical ordering $<$ on $\Gamma := \{X_1^{d_1}\cdots X_n^{d_n}Y_1^{e_1}\cdots Y_m^{e_m} | (d_1,\dots,d_n,e_1,\dots,e_m) \in \mathbb{N}^{n+m}\}$ induced by $X_1 < \ldots < X_n < Y_1 < \ldots < Y_m$ where a_{ij}, b_{jl}, c_{lk} are invertible elements in $\mathscr{R}$,
$v_{jl} \in \{X_1^{d_1}\cdots X_j^{d_j} \mid (d_1,\dots,d_j) \in \mathbb{N}^j\}$ $d_{ij}, e_{jl}, f_{lk} \in \mathscr{A}$ with $\mathbf{T}(d_{ij}) < X_iX_j$, $\mathbf{T}(e_{jl}) < X_jY_l$, $\mathbf{T}(f_{lk}) < Y_kY_l$. The associated graded ring $\mathscr{G}$ is obtained by setting $d_{ij} = e_{jl} = f_{lk} = 0$. We immediately remark that, unless we restrict to the case in which each $v_{jl} = \mathbf{1}_{\mathscr{A}}$, noetherianity is not sufficient to grant termination and finiteness.

Example 1 Simply consider Tamari's [23] ring $\mathbb{Q}\langle X,Y\rangle/\mathbb{I}(YX - X^2Y)$ where the principal ideal $\mathscr{I} = (X)$ has the infinite involutive basis $\{X^{2^i}Y^i, i \in \mathbb{N}\}$ each element having X as multiplicative variable.

Under this restriction, we obtain in any case a class of rings larger than solvable polynomial rings‡ even if $\mathscr{R}$ is assumed to be a field; there are in fact for each term $\tau \in \Gamma$ an automorphism $\alpha_\tau : \mathscr{R} \to \mathscr{R}$ and for each two terms $\tau_1,\tau_2 \in \Gamma$ an element $\varpi(\tau_2,\tau_1) \in \mathscr{R}$ so that the multiplicative $*$ arithmetic of $\mathscr{G}$ is defined by distributing the monomial product

$$a_1\tau_1 * a_2\tau_2 = a_i\alpha_{\tau_1}(a_2)\varpi(\tau_1,\tau_2)\tau_1 \circ \tau_2$$

†Up to Second Buchberger Criterion [3] but probably including the other criteria proposed by Gebauer and Möller [8].

‡where each α_τ is the identity and each $\varpi(\tau_2,\tau_1) = 1$ so that $a_1\tau_1 * a_2\tau_2 = a_1a_2\tau_1 \circ \tau_2$.

where $\circ$ denote the classical multiplication in Γ. Already under this restriction and even assuming $\mathcal{R}$ to be a field, the classical

Theorem 2 [9,Th.4.10, 10, Th.2.10] If an involutive division is left(/right/restricted) continuous then left(/right/restricted) local involutivity of any set U implies its left(/right/restricted) involutivity.

is not obvious [7]: it can be proved by means of Jacobi-like formulas which can be deduced on effective rings via associativity. The main problem arises when the coefficient ring $\mathcal{D}$, on which $\mathcal{R} = \mathcal{D}\langle\overline{\mathbf{v}}\rangle / I$ is a module, is not a field but just a PID[††]; as it was remarked by Seiler [22] one needs at least to follow the standard approach in Buchberger Theory and speak of *weak* and *strong* bases.

Example 3 [20] In the ideal $\mathcal{I} := \mathbb{I}(g_1, g_2) \subset \mathbb{Z}[X, Y]$, $g_1 := 3X$, $g_2 := 2Y$, it holds $\mathcal{I} \ni g_3 := XY = g_1 Y - g_2 X$ while $3X \nmid XY$ and $2Y \nmid XY$. As a consequence the characterization of a set U to be *involutive/complete with respect to an involutive division* L which in the field case [9,Def.4.1] [10,Def.2.4] simply requires $\cup_{u\in U} u L(u, U) = \cup_{u\in U} u\Gamma \subset \Gamma$ must be reconsidered since we should require a formulation $\cup_{u\in U} u L(u, U) = \cup_{u\in U} u \mathsf{M}(\mathcal{A}) \subset \mathsf{M}(\mathcal{A}) := \{ct : t \in \Gamma, c \in \mathcal{R} \setminus \{0\}\}$ but, in general $\mathcal{N} := \cup_{u\in U} u \mathsf{M}(\mathcal{A}) \subsetneq \mathbb{I}(U) \cap \mathsf{M}(\mathcal{A}) = \mathrm{Span}_{\mathcal{R}}\{\mathcal{N}\} \cap \mathsf{M}(\mathcal{A})$. For the moment we have postponed the investigation of the *strong* case and we [7] have adapted the terminology from the *terms* Γ with coefficients over a field to the *monomials* $\mathsf{M}(\mathcal{A})$, the coefficients being over an effectively given ring $\mathcal{R}$ and applied *Weispfenning multiplication* [24,5] in order to deduce twosided (and subbilateral) bases from restricted ones, but mainly we have considered only the easiest *weak* case. In this setting, of course, we loose one stength of involutiveness, namely that any monomial $w \in \mathsf{M}(\mathcal{A})$ has at most one $L-$involutive divisor in U, a property which can be granted, via *strong* bases, only when $\mathcal{R}$ itself is a PIR. Therefore reduction of a monomial $c\tau \in \mathsf{M}(\mathcal{A})$ must be performed considering all potential divisors $c_i\tau_i \in U$ such that $\tau_i \mid \tau$, $\tau = \upsilon_i \circ \tau_i$ and looking for relations $c = \sum_i a_i \alpha_{\upsilon_i} \varpi(\upsilon_i, \tau_i)$ and reduction be performed via classical Buchberger reduction. In the *strong* cases, on the basis of [20,14,19], we guess that the test/completion for involutivity of a continuous involutive division, which in the field case (Theorem) is local involutivity, should be reformulated as

Claim 4 [10, Th.6.5] Let L be a continuous involutive division. A polynomial set F is strong L-involutive if

• for each $f \in F$ and each non-multiplicative variable $x \in NM_L(lc(f), lc(F))$, the related J-prolongation $f \cdot x_i$,

•for each $f, g \in F$ the related P-prolongation $s\frac{lcm(\mathbf{T}(f),\mathbf{T}(g))}{\mathbf{T}(f)} f + t\frac{lcm(\mathbf{T}(g)g,\mathbf{T}(g))}{\mathbf{T}(f)}$, where c, s are the Bezout values such that $slc(f) + tlc(g) = \gcd(lc(f), lc(g)$,

•for each $f \in F$ the related A-prolongation af, a being the annihilator of $lc(f)$

reduce all of them to zero modulo F.

There is still some research required in the strong case when $\mathcal{R}$ itself is PID; we need to investigate whether both the classical [9,10] approach and the recent RID [4] suggestion are able to recover the division structure of polynomial domains.

[††]the PIR case simply requires to deal with proper annihilators.

Example 5 For the ideal $\mathscr{I} := \mathbb{I}\left(8X, 4X^3, 2X^6, 36Y^2, 6Y^3, Y^4\right) \subset \mathbb{Z}[X,Y]$ a (minimal) strong Gröbner basis is $\bar{U} := \{8X, 4X^3, 2X^6, 36Y^2, 4XY^2, 6Y^3, 2XY^3, Y^4\}$; with respect the Janet/Pommaret division a strong minimal involutive basis is

$$\begin{aligned}\tilde{U} &:= \left\{8X^{1+i}Y^j, 0 \le i \le 1, 0 \le j \le 1\right\} \cup \left\{4X^{3+i}Y^j, 0 \le i \le 2, 0 \le j \le 1\right\}\\ \cup &\quad \left\{2X^6Y^j, 0 \le j \le 3\right\} \cup \left\{36Y^2, 6Y^3, Y^4\right\} \cup \left\{4X^{1+i}Y^2, 0 \le i \le 4\right\} \cup \left\{2X^{1+i}Y^3, 0 \le i \le 4\right\}\end{aligned}$$

τ	$M(\tau)$	$NM(\tau)$
Y^4	$\{X,Y\}$	$\emptyset$
$\left\{2X^6Y^j, 0 \le j \le 3\right\}$	$\{X\}$	$\{Y\}$
$\emptyset$	$\{Y\}$	$\{X\}$
$\tilde{U} \setminus \{2X^6, 2X^6Y, 2X^6Y^2, 2X^6Y^3, Y^4\}$	$\emptyset$	$\{X,Y\}$

Keywords
Weak Involutive bases, effective rings, Weispfenning multiplication

References

[1] Buchberger B., *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph. D. Thesis, Innsbruck (1965)
[2] Buchberger B., *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleischunssystem*, Aeq. Math. **4** (1970), 374–383
[3] Buchberger B., *A Criterion for Detecting Unnecessary Reduction in the Construction of Gröbner bases*, L. N. Comp. Sci **72** (1979), 3–21, Springer
[4] Ceria, M., *Combinatorial decompositions for monomial ideals*, preprint
[5] Ceria, M., Mora, T. *Buchberger-Weispfenning Theory for Effective Associative Rings*, J. Symb. Comp., special issue for ISSAC 2015, 83, pp. 112-146.
[6] Ceria, M., Mora, T., *Buchberger-Zacharias Theory of Multivariate Ore Extensions*, Journal of Pure and Applied Algebra Volume 221, Issue 12, December 2017, Pages 2974-3026
[7] Ceria, M., Mora, T. *Weak Involutive bases over effective rings*, submitted to ISSAC2019
[8] Gebauer R., Möller H.M., *A fast Variant of Buchbgerger's Algorithm*, Preprint (1985)
[9] Gerdt V.P., Blinkov Y.A. *Involutive bases of Polynomial Ideals*, Math. Comp. Simul. **45** (1998), 543–560
[10] Gerdt V.P., Blinkov Y.A. *Minimal involutive bases*, Math. Comp. Simul. **45** (1998), 519–541
[11] Janet M. , *Sur les systèmes d'équations aux dérivées partielles* J. Math. Pure et Appl., **3** (1920), 65–151
[12] Kandri-Rody, A., Weispfenning, W., *Non-commutative Gröbner Bases in Algebras of Solvable Type*, J. Symb. Comp. **9** (1990), 1–26
[13] Ore O., *Theory of non-commutative polynomials* , Ann. Math. **34** (1933), 480–508
[14] Möller H.M., *On the construction of Gröbner bases using syzygies*, J. Symb. Comp. **6** (1988), 345–359

[15] T. Mora, *Solving Polynomial Equation Systems* 4 Vols., Cambridge University Press, I (2003), II (2005), III (2015), IV (2016)
[16] T. Mora, *Zacharias Representation of Effective Associative Rings*
[17] F. Mora, *De Nugis Groebnerialium 4: Zacharias, Spears, Möller* Proc. ISSAC'15 (2015), 191–198, ACM
[18] B. Nguefack, E. Pola, *Effective Buchberger-Zacharias-Weispfenning theory of skew polynomial extensions of restricted bilateral coherent rings*, J. Symb. Comp.
[19] Norton G.H., Sălăgean A., *Strong Gröbner bases for polynomials over a principal ideal ring*, Bull. Austral. Math. Soc. **64** (2001), 505–528
[20] Pan L., *On the D-bases of polynomial ideals over principal ideal domains,* J. Symb. Comp. **7** (1988), 55–69
[21] Schwartz F., *Reduction and Completion Algorithm for Partial Differential Equations*, Proc. ISSAC'92 (1992), 49–56 ACM
[22] Seiler W.M. *A Combinatorial Approach to Involution and δ-Regularity I: Involutive Bases in Polynommial Algebras of Solvable Type* J. AAECC **20** (2009), 207–259
[23] Tamari D. *On a certain Classification of rings and semigroups* Bull. A.M.S. **54** (1948), 153–158.
[24] Weispfenning, V. *Finite Gröbner bases in non-noetherian Skew Polynomial Rings* Proc. ISSAC'92 (1992), 320–332, A.C.M.

Modular methods for rich algebraic geometry results on hyperplane arrangements

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

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

1 Hyperplane arrangements

Let K be a field. A finite set of affine hyperplanes $\mathscr{A} = \{H_1,\dots,H_n\}$ in K^l is called a *hyperplane arrangement*. For each hyperplane H_i we fix a defining polynomial $\alpha_i \in S = S^*(K^l) = K[x_1,\dots,x_l]$ such that $H_i = \alpha_i^{-1}(0)$, and let $Q(\mathscr{A}) := \prod_{i=1}^n \alpha_i$. An arrangement $\mathscr{A}$ is called *central* if each H_i contains the origin of K^l.

We denote by $\mathrm{Der}_{K^l} := \{\sum_{i=1}^l f_i\partial_{x_i} \mid f_i \in S\}$ the S-module of *polynomial vector fields* on K^l (or S-derivations). Let $\delta = \sum_{i=1}^l f_i\partial_{x_i} \in \mathrm{Der}_{K^l}$. Then δ is said to be *homogeneous* of polynomial degree d if $f_1,\dots,f_l$ are homogeneous polynomials of degree d in S. In this case, we write $\mathrm{pdeg}(\delta) = d$.

A central arrangement $\mathscr{A}$ is said to be *free* with exponents $(e_1,\dots,e_l)$ if and only if the module of vector fields logarithmic tangent to $\mathscr{A}$,

$$D(\mathscr{A}) := \{\delta \in \mathrm{Der}_{K^l} \mid \delta(\alpha_i) \in \langle\alpha_i\rangle S, \forall i\},$$

is a free S-module and there exists a basis $\delta_1,\dots,\delta_l \in D(\mathscr{A})$ such that $\mathrm{pdeg}(\delta_i) = e_i$, or equivalently $D(\mathscr{A}) \cong \bigoplus_{i=1}^l S(-e_i)$.

The module $D(\mathscr{A})$ is a graded S-module and $D(\mathscr{A}) = \{\delta \in \mathrm{Der}_{K^l} \mid \delta(Q(\mathscr{A})) \in \langle Q(\mathscr{A})\rangle S\}$. In particular, since the arrangement $\mathscr{A}$ is central, then the Euler vector field $\delta_E := \sum_{i=1}^l x_i\partial_{x_i}$ belongs to $D(\mathscr{A})$. If the characteristic of K does not divide n, then $D(\mathscr{A}) \cong S\cdot\delta_E \oplus D_0(\mathscr{A})$, where $D_0(\mathscr{A}) := \{\delta \in \mathrm{Der}_{K^l} \mid \delta(Q(\mathscr{A})) = 0\}$.

In general the exponents of an arrangement depend on the characteristic of K. In fact, we have Example 4.35 from [3].

Example 1.1. *Consider the arrangement $\mathscr{A}$ in K^3 with $Q(\mathscr{A}) = xyz(x-y)(x+z)(y+z)(x+y+z)$. Then $\mathscr{A}$ is free for any K, but its exponents depend on the characteristic of K.*

If the characteristic of K is different from 2, then $\mathscr{A}$ is free with exponents $(1,3,3)$, in fact we can take as basis of $D(\mathscr{A})$ the following vector fields δ_E, $\delta_2 = x(x+z)(x+y+z)\partial_x + y(y+z)(x+y+z)\partial_y$ and $\delta_3 = x(x+z)(2y+z)\partial_x + y(y+z)(2x+z)\partial_y$.

If the characteristic of K is 2, then $\mathscr{A}$ is free with exponents $(1,2,4)$, in fact we can take as basis of $D(\mathscr{A})$ the following vector fields δ_E, $\delta_2 = x^2\partial_x + y^2\partial_y + z^2\partial_z$ and $\delta_3 = x^4\partial_x + y^4\partial_y + z^4\partial_z$.

One of the most famous characterization of freeness is due to Terao [6] and it uses $J(\mathscr{A})$ the *Jacobian ideal* of $\mathscr{A}$, i.e. the ideal of S generated by $Q(\mathscr{A})$ and its partial derivatives.

Theorem 1.2. *A central arrangement $\mathscr{A}$ in K^l is free if and only if $S/J(\mathscr{A})$ is 0 or $(l-2)$-dimensional Cohen-Macaulay.*

2 Change of characteristic

In [4], we studied the connections between freeness over a field of characteristic zero and over a finite field. All the computations were done using the computer algebra system CoCoA [1], and the new package `arrangements` [5].

Assume that $\mathscr{A} = \{H_1,\dots,H_n\}$ is a central arrangement in $\mathbb{Q}^l$. After clearing denominators, we can suppose that $\alpha_i \in \mathbb{Z}[x_1,\dots,x_l]$ for all $i = 1,\dots,n$, and hence that $Q(\mathscr{A}) = \prod_{i=1}^n \alpha_i \in \mathbb{Z}[x_1,\dots,x_l]$. Moreover, we can also assume that there exists no prime number p that divides any α_i.

Let p be a prime number. Consider the image of $Q(\mathscr{A})$ under the canonical homomorphism

$$\pi_p \colon \mathbb{Z}[x_1,\dots,x_l] \to \mathbb{F}_p[x_1,\dots,x_l].$$

If $\pi_p(Q(\mathscr{A}))$ is reduced, we will say that the prime number p is *good* for $\mathscr{A}$. Notice that there is a finite number of primes p that are not good for $\mathscr{A}$.

Let now p be a good prime for $\mathscr{A}$, and consider $\mathscr{A}_p$ the arrangement in $\mathbb{F}_p^l$ defined by $\pi_p(Q(\mathscr{A}))$. Hence, by construction, $Q(\mathscr{A}_p) = \pi_p(Q(\mathscr{A})) \neq 0$ and it is reduced.

Theorem 2.1. *If $\mathscr{A}$ is free in $\mathbb{Q}^l$ with exponents $(e_1,\dots,e_l)$, then $\mathscr{A}_p$ is free in $\mathbb{F}_p^l$ with exponents $(e_1,\dots,e_l)$, for all good primes except possibly a finite number of them.*

Example 2.2. *Consider $\mathscr{A}$ the arrangement in $\mathbb{Q}^4$ as the cone of $\mathscr{A}^{[-2,2]}$ the Shi-Catalan arrangement of type B. As described in [2], $\mathscr{A}$ is free with exponents $(1,13,15,17)$. Now, $5,7$ and 11 are all good prime numbers for $\mathscr{A}$. A direct computation shows that the arrangement $\mathscr{A}_5$ over $\mathbb{F}_5$ is free with exponents $(1,5,15,25)$. However, both $\mathscr{A}_7$ over $\mathbb{F}_7$ and $\mathscr{A}_{11}$ over $\mathbb{F}_{11}$ are not free. Moreover, for any other good prime number p, $\mathscr{A}_p$ over $\mathbb{F}_p$ is free with exponents $(1,13,15,17)$.*

Since the number of not good primes for $\mathscr{A}$ is finite, we have the following.

Corollary 2.3. *Let $\mathscr{A}$ be a central arrangement in $\mathbb{Q}^l$ and p a large prime number. If $\mathscr{A}$ is free in $\mathbb{Q}^l$ with exponents $(e_1,\dots,e_l)$, then $\mathscr{A}_p$ is free in $\mathbb{F}_p^l$ with exponents $(e_1,\dots,e_l)$.*

Denote by $J(\mathscr{A})_{\mathbb{Z}}$ the ideal of $\mathbb{Z}[x_1,\dots,x_l]$ generated by $Q(\mathscr{A})$ and its partial derivatives.

Lemma 2.4. *The number of distinct primes that are zero divisors in $\mathbb{Z}[x_1,\dots,x_l]/J(\mathscr{A})_{\mathbb{Z}}$ is finite. Moreover, these zero divisors can be computed via the computation of a minimal strong Gröbner basis of $J(\mathscr{A})_{\mathbb{Z}}$.*

Theorem 2.5. *Let $\mathscr{A}$ be a central arrangement in $\mathbb{Q}^l$. Let p be a good prime number for $\mathscr{A}$ that does not divide n and that is a non-zero divisor in $\mathbb{Z}[x_1,\dots,x_l]/J(\mathscr{A})_\mathbb{Z}$. If $\mathscr{A}_p$ is free in $\mathbb{F}_p^l$ with exponents $(e_1,\dots,e_l)$, then $\mathscr{A}$ is free in $\mathbb{Q}^l$ with exponents $(e_1,\dots,e_l)$.*

In Theorem 2.5, the assumption that the prime p is a non-zero divisor in $\mathbb{Z}[x_1,\dots,x_l]/J(\mathscr{A})_\mathbb{Z}$ is fundamental. In fact we have the following.

Example 2.6. *Consider the arrangement $\mathscr{A} \subseteq \mathbb{Q}^3$ with defining polynomial $Q(\mathscr{A}) = z(x+2y-4z)(y+4z)(x+3y-6z)$. Both $\mathscr{A}_2$ and $\mathscr{A}_3$ are free with exponents $(1,1,2)$. However, $\mathscr{A}$ is not free but this does not contradict Theorem 2.5 because both 2 and 3 are zero divisors in $\mathbb{Z}[x_1,\dots,x_l]/J(\mathscr{A})_\mathbb{Z}$. In fact, we have that $3(y^2z^2+2yz^3-8z^4) \in J(\mathscr{A})_\mathbb{Z}$ but $y^2z^2+2yz^3-8z^4 \notin J(\mathscr{A})_\mathbb{Z}$, and similarly $2(xyz^2+4y^2z^2+4xz^3+8yz^3-32z^4) \in J(\mathscr{A})_\mathbb{Z}$ but $xyz^2+4y^2z^2+4xz^3+8yz^3-32z^4 \notin J(\mathscr{A})_\mathbb{Z}$.*

By Lemma 2.4, the number of prime numbers that are zero divisors in $\mathbb{Z}[x_1,\dots,x_l]/J(\mathscr{A})_\mathbb{Z}$ is finite. Hence, putting together Corollary 2.3 and Theorem 2.5, we have the following.

Corollary 2.7. *Let $\mathscr{A}$ be a central arrangement in $\mathbb{Q}^l$ and p a large prime number. $\mathscr{A}_p$ is free in $\mathbb{F}_p^l$ with exponents $(e_1,\dots,e_l)$ if and only if $\mathscr{A}$ is free in $\mathbb{Q}^l$ with exponents $(e_1,\dots,e_l)$.*

Example 2.8. *Consider the arrangement $\mathscr{A}$ in $\mathbb{Q}^3$ with defining polynomial $Q(\mathscr{A}) = xyz(x-y)(x+y)(x-z)(x+z)(y-z)(y+z)$. Now, $p=5$ is a good prime number for $\mathscr{A}$ that does not divide $|\mathscr{A}|=9$ and that is a non-zero divisor in $\mathbb{Z}[x,y,z]/J(\mathscr{A})_\mathbb{Z}$. A direct computations shows that $\mathscr{A}$ and $\mathscr{A}_5$ are free with exponents $(1,3,5)$. Notice that in this case, $\mathscr{A}$ and $\mathscr{A}_5$ have isomorphic intersection lattice, hence $p=5$ is a "large prime number". However, in general, it is difficult to detect when a prime number is "large" enough.*

Keywords
Hyperplane Arrangements, Freeness, Modular Methods

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] T. ABE; H. TERAO, The freeness of Shi–Catalan arrangements. *European Journal of Combinatorics* **32**(8), 1191–1198 (2011).
[3] P. ORLIK; H. TERAO, *Arrangements of hyperplanes.* Springer-Verlag, Berlin, 1992.
[4] E. PALEZZATO; M. TORIELLI, Free hyperplane arrangements over arbitrary fields. Available at *arXiv:1803.09908.*
[5] E. PALEZZATO; M. TORIELLI, Hyperplane arrangements in CoCoA. To appear on *Journal of Software for Algebra and Geometry.*
[6] H. TERAO, Arrangements of hyperplanes and their freeness I. *J. Fac. Sci. Univ. Tokyo Sect. IA Math* **27**(2), 293–312 (1980).

A dynamic F4 algorithm

John Perry[1] [john.perry@usm.edu]

[1] School of Mathematics and Natural Sciences, University of Southern Mississippi, Hattiesburg, MS

Gröbner bases of polynomial ideals are a fundamental tool of computational commutative algebra, and by extension a tool of applied computer algebra. The past half-century has seen steady progress in the development of algorithms to compute Gröbner bases, with some of the better-known algorithms being Buchberger's algorithm [1] and Faugère's algorithms F4 and F5 [4, 5]. The latter are well-known for their utility in algebraic cryptanalysis [6, 7].

The "Gröbner property" depends on how one orders the polynomials' terms, so a set of polynomials can be a Gröbner basis with respect to one term ordering, but not with respect to another. (For instance, $\{x+y, y^2+1\}$ is a Gröbner basis when $x > y$, but not when $y > x$.) Thus, while an ideal's "reduced Gröbner basis" is completely determined once we settle on a term ordering, most ideals have more than one reduced Gröbner basis, depending on which ordering we choose. Indeed, the choice of ordering can have a significant effect on the number of polynomials that appear in an ideal's reduced Gröbner basis.

Many applications require only a Gröbner basis' leading terms, so if a basis with respect to one ordering contains only 400 polynomials, while a basis with respect to another contains 1300, we might well prefer the first basis, *even if the computation took a little longer*. For certain applications, one might prefer an ideal-specific term ordering [11], but in general, experience shows quickly that some orderings generally produce smaller bases more quickly than others (though this is not always the case).

In any case, these approaches are "static", insofar as they require as input both an ideal's generators and a monomial ordering, and compute a Gröbner basis *with respect to the given ordering*. (All major computer algebra systems employ this approach.) A quarter century ago, some researchers proposed a "dynamic" approach [2, 8] which would require only the ideal's generators as input, then compute *both* a monomial ordering *and* a Gröbner basis with respect to that ordering. Desired constraints on the ordering translate naturally into a system of linear inequalities, which the simplex method can solve quickly and easily, obtaining a weighted ordering: the constraint $x_0 > x_1^2$ corresponds to $\{\omega_i > 0, \omega_0 - 2\omega_1 > 0\}$, with ω the weight vector. Via a reasonable heuristic, algorithms that use the dynamic approach select orderings that very often produce a basis with fewer polynomials than a static algorithm using the customary, graded reverse lexicographic ordering — and sometimes do so faster.

Recent work in this area has focused on simplifying the system of linear inequalities and exploring other heuristics [3, 9, 10]. However, all this work has taken place in the context of a dynamic Buchberger algorithm. One naturally wonders how a dynamic F4 algorithm would behave, especially in the context of parallel computation.

This talk describes one such dynamic F4 implementation, built from scratch using C++11 and the Standard Template Library, in particular its `threads` library. It will also consider the related question of identifying terms that cannot possibly be a polynomial's leading term. Identifying such terms allows us to reduce the number of inequalities needed to check for feasibility, so it is clearly an important consideration for a dynamic approach. Already [2] used the fact that if t, u are monomials and t divides u, then $u > t$ regardless of the term ordering, and [3] used the extreme vectors of the linear inequalities' solution cone to describe a technique that identified additional incompatible terms. We consider an attempt to optimize this technique, as well as a new criterion to identify monomials that cannot possibly be leading terms.

Keywords
Gröbner bases, F4, dynamic algorithms

References

[1] B. BUCHBERGER, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalem Polynomideal (An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal)*. Mathematical Institute, University of Innsbruck, 1965.
English translation published in the Journal of Symbolic Computation (2006) 475–511.
[2] M. CABOARA, A Dynamic Algorithm for Gröbner basis computation. In *ISSAC '93*, Manuel Bronstein (ed.), 275–283. ACM Press, New York, 1993.
[3] M. CABOARA; J. PERRY, Reducing the size and number of linear programs in a dynamic Gröbner basis algorithm. *Applicable Algebra in Engineering, Communication and Computing* **25**(1), 99–117 (2014).
[4] J-C FAUGÈRE, A New Efficient Algorithm for Computing Gröbner bases (F4). *Journal of Pure and Applied Algebra* **139**(1–3), 61–88 (1999).
[5] J-C FAUGÈRE, A new efficient algorithm for computing Gröbner bases without reduction to zero F5. In *ISSAC '02*, Marc Giusti (ed.), 75–82. ACM Press, New York, 2002.
[6] J-C FAUGÈRE, Cryptochallenge 11 is broken or an efficient attack of the C* cryptosystem. Technical report, LIP6/Universitè Paris, 2005.
[7] J-C FAUGÈRE, Algebraic cryptanalysis of mceliece variants with compact keys. In *EUROCRYPT'10*, Henri Gilbert (ed.), 279–298. Springer-Verlag Berlin, Heidelberg, 2010.
[8] P. GRITZMANN; B. STURMFELS, Minkowski Addition of Polytopes: Computational Complexity and Applications to Gröbner Bases. *SIAM J. Disc. Math* **6**(2), 246–269 (1993).
[9] G. LANGELOH, *Unrestricted dynamic Gröbner Basis algorithms*. Master's thesis, Universidade Federal do Rio Grande do Sul, 2019.
[10] J. PERRY, Exploring the Dynamic Buchberger Algorithm. In *ISSAC'17*, Michael Burr (ed.), 365–372. ACM Press, New York, 2017.
[11] Q-N TRAN, Ideal-Specified Term Orders for Elimination and Applications in Implicitization. In *Proceedings of the Tenth International Conference on Applications of Computer Algebra*, Quoc-Nam Tran and Franz Winkler (ed.), 15–24. ACA Press, 2004.

Rational reparametrization of polynomial ODEs, PDEs and linear systems with radical coefficients

***Jorge Caravantes*[1], *J. Rafael Sendra*[1], *David Sevilla*[2], *Carlos Villarino*[1]** [sevillad@unex.es]

[1] Department of Physics and Mathematics, University of Alcalá, Spain
[2] Department of Mathematics, University of Extremadura, Spain

For solving certain classes of differential equations, one can take advantage of algorithms in Algebraic Geometry. Our goal is to expand on some of those results [1,2], which make use of the fact that one can parametrize rationally certain algebraic objects associated to those equations.

In particular, here we apply constructive techniques of reparametrization of algebraic varieties to the following problem: given a ODE of the form $F(y(x), y'(x), y''(x), \ldots) = 0$ where F is a polynomial whose coefficients are radical functions in x, find, if it exists, an equivalent ODE (that is, given by an invertible reparametrization $x = r(z)$) to obtain $G(Y(z), Y'(z), Y''(z), \ldots) = 0$ such that the coefficients of G are rational functions in x (the new equation is called *algebraic*). For example:

Example Consider the ODE $\sqrt{x}\,y''(x) + \sqrt{x+1} + x = 0$. The change of variable $x = \frac{z^4-2z^2+1}{4z^2}$ converts the original ODE into

$$\frac{2z^5 Y''(z)}{(z-1)(z+1)(z^2+1)^2} - \frac{2z^4(z^4+3)\,Y'(z)}{(z^2+1)^3(z-1)^2(z+1)^2} + \frac{z^4+2z^3-2z^2+2z+1}{4z^2} = 0$$

which is algebraic as expected. The inverse change is $z = \sqrt{x+1} + \sqrt{x}$, allowing us to recover solutions of the original equation by solving the second one.

We present similar results for the case of PDEs and of linear systems of ODEs/PDEs.

Our approach is based on our previous work on parametrization of nonrational varieties [3]. In particular, we construct a radical parametric algebraic variety of the same dimension as the number of variables (i.e. for ODEs we work with curves) and analyze whether it can be reparametrize it without radicals.

We construct an auxiliary variety that encapsulates the relevant information about the nonrationality of the radical variety associated to the ODEs. The construction is based on a tower of radical extensions where the coefficients of the ODE are, and so the auxiliary variety is called the *tower variety*. In those instances where algorithms for parametrization of algebraic varieties exist (for example, for curves), a rational parametrization of the tower variety provides a reparametrization of the radical variety that is rational, and this in turn provides the change of variable that converts the ODE with radical coefficients into another one with rational coefficients, to which the techniques mentioned in the beginning may be applied.

Definition. Let $\mathbb{F}_m$ be the last field in a tower of radical extensions of $\mathbb{C}(x)$. That is,

$$\mathbb{F}_0 = \mathbb{C}(x) \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_m$$

where $\mathbb{F}_i = \mathbb{F}_{i-1}(\delta_i)$, each δ_i being the root of an element in the previous field: $\delta_i^{e_i} \in \mathbb{F}_{i-1}$.

Then, the *tower variety* of a parametrization $\mathscr{P}$ whose components are in $\mathbb{F}_m$ is the Zariski closure of the (non-rational) map $x \mapsto (x, \delta_1(x), \ldots, \delta_m(x))$. It depends on the elements defining the tower, but useful properties are proven for any such choices.

Theorem. With the notation of the previous definition, Let $a_1(x), \ldots, a_k(x) \in \mathbb{F}_m$ be the coefficients of the given ODE in any order, and let $\mathcal{V}_{\mathscr{P}}$ the Zariski closure of the image of the map $\mathscr{P}\colon x \mapsto (a_1(x), \ldots, a_k(x)) \in \mathbb{C}^k$. Let $\mathcal{V}_{\mathbb{T}}$ be the tower variety of $\mathscr{P}$.

Then:

1. If $\mathcal{V}_{\mathbb{T}}$ is rational then $\mathcal{V}_{\mathscr{P}}$ is rational.
2. If $\mathscr{Q}(z) = (r(z), \ldots)$ is a rational parametrization of $\mathcal{V}_{\mathbb{T}}$, then the ODE obtained with the change of variable $x = r(z)$ is algebraic.
3. Suppose that $\mathscr{Q}(z)$ above is invertible and let $h(\overline{z})$ be its inverse. If $Y(z)$ is a solution of the ODE obtained in the previous item, then $Y(h(x, \overline{\delta}(x)))$ is a solution of the original ODE, where $\overline{\delta}(x)$ is the tuple of radicals involved in the construction.

Similar results apply to the case of PDEs. Also to linear systems of ODEs in unknowns $y_1(x), \ldots, y_m(x)$, and even to nonlinear (polynomial) systems as long as no term of any equation contains a product of y_i, y_j, $i \neq j$ or their derivatives.

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 third author is a member of the GADAC group and is partially supported by Junta de Extremadura and Fondo Europeo de Desarrollo Regional (GR18001).

Keywords
Ordinary differential equation, Partial differential equation, Algebraic curve, Reparametrization, Radical parametrization

References
[1] G. GRASEGGER; F. WINKLER, Symbolic solutions of first-order algebraic ODEs. In *Computer algebra and polynomials, volume 8942 of Lecture Notes in Comput. Sci.*, Jaime Gutierrez, Josef Schicho, and Martin Weimann (eds.), 94–104. Springer, 2015.
[2] G. GRASEGGER; N. THIEU VO; F. WINKLER, Deciding the existence of rational general solutions for first-order algebraic odes. *J. of Symb. Comp.* **87**, 127–139 (2018).

[3] J. R. SENDRA; D. SEVILLA; C. VILLARINO, Algebraic and algorithmic aspects of radical parametrizations. *Comput. Aided Geom. Design* **55**, 1–14 (2017).
[4] J. R. SENDRA; D. SEVILLA; C. VILLARINO, Rational reparametrization of ODEs with radical coefficients. In *Monografías de la Real Academia de Ciencias (proceedings of EACA 2018)*, E. Artal and J.I. Cogolludo (eds.), 135–138. 2018.

Algorithms for Polynomials in Legendre-Sobolev Bases

Parisa Alvandi[1] **,** ***Stephen M. Watt***[1] [smwatt@uwaterloo.ca]

[1]David R. Cheriton School of Computer Science, University of Waterloo, Canada N2L 3G1

Earlier work [1] has shown how handwritten characters may be represented as plane curves with $x(\lambda)$ and $y(\lambda)$ polynomial functions, and how efficient recognition can be achieved when the polynomials are written in a Legendre-Sobolev (LS) basis. It is therefore interesting to be able to perform various symbolic-numeric polynomial operations directly in LS bases. We find it is sufficient to work with basis polynomials orthogonal with respect to inner products of the form studied by Althammer [2],

$$\langle f, g\rangle = \int_{-1}^{1} f(\lambda)g(\lambda)\mathrm{d}\lambda + \mu\int_{-1}^{1} f'(\lambda)g'(\lambda)\mathrm{d}\lambda,\ \mu \geq 0$$

We show how functional approximations may be constructed from moments integrated in real time, how to compute derivatives, roots and polynomial GCD in LS bases by linear algebra methods.

Keywords
symbolic-numeric algorithms, polynomial algebra, Legendre-Sobolev polynomials, mathematical handwriting recognition

References

[1] O. GOLUBITSKY, S.M. WATT, Distance-Based Classification of Handwritten Symbols. *Int. J. Doc. Anal. and Recog.* **13**(2), 133–146 (2010).
[2] P. ALTHAMMER, Eine Erweiterung des Orthogonalitätsbegriffes bei Polynomen und deren Anwendung auf die beste approximation. *J. Reine Ang. Math.* **211**, 192–204 (1962).

Computing the genus of plane curves with cubic complexity in the degree

***A. Poteaux*[1], *M. Weimann*[2]** [martin.weimann@upf.pf]

[1]CRIstal, University of Lilles, France
[2] GAATI, University of French Polynesia

In this presentation, we report on new complexity results about the resolution of singularities of plane curves, obtained in collaboration with Adrien Poteaux in [9] and [10]. Let C be an absolutely irreducible algebraic plane curve defined over a perfect field $\mathbb{K}$ of characteristic 0 or greater than $d = \deg(C)$. We will sketch the proof of the following result [9, Cor. 1]:

Theorem 1. *There exists an algorithm which computes the geometric genus of C with an expected $\tilde{\mathcal{O}}(d^3)$ arithmetic operations over $\mathbb{K}$.*

If $\mathbb{K} = \mathbb{Q}$, we can use a criterion of good reduction modulo p [7] and derive a Las Vegas algorithm for the genus running with an expected *bit* complexity $\tilde{\mathcal{O}}(d^3(h+1))$ where h stands for the logarithmic height of a polynomial equation of C over $\mathbb{Q}$ (similar results stand over arbitrary number fields, see [9]). Our approach uses Puiseux series. There exist other algorithms for the genus, using for instance linear differential operators [2, 3] or topological methods [5] (for complex curves). To our knowledge, none of these methods have been proved to provide a better complexity than that of Theorem 1.

The proof of Theorem 1 is based on a fast Newton-Puiseux type algorithm. If $F \in \mathbb{K}[[x]][y]$ is a square-free polynomial defined over a perfect field $\mathbb{K}$ of characteristic 0 or greater than $d = \deg(F)$, the roots of F in $\overline{\mathbb{K}((x))}$ may be represented as fractional Puiseux series. Computing these Puiseux series is an important algorithmic issue related to algebraic curves with various applications (resolution of singularities, integral basis of function fields, Riemann-Roch spaces, monodromy, factorization, geometric modeling, etc). An important fact in our context is that the singular parts of the Puiseux series (obtained after truncation up to a suitable power of x) contain the classical numerical invariants attached to the singular germs of plane curve defined by F along the line $x = 0$. In particular, they determine their equisingularity type, which is the main notion of equivalence for plane curve singularities introduced by Zariski in the 60's. Denoting δ the x-valuation of the discriminant of F, we prove [9, Thm.1]:

Theorem 2. *There exists an algorithm which computes the singular parts of the Puiseux series of F with an expected $\tilde{\mathcal{O}}(d\delta)$ arithmetic operations over $\mathbb{K}$.*

When compared to the Newton-Puiseux type algorithms of Duval [4] and Poteaux-Rybowicz [7,8], the new idea behind the proof of Theorem 2 is to use a divide and conquer strategy. To this aim, we use suitable sharp truncation bounds (updated at each step of the algorithm) combined with a generalization of the classical Hensel lifting. Also, we need to rely on dynamic evaluation in order to avoid to perform too many univariate irreducibility tests (this task is too costly over characteristic zero fields and might be too costly also for finite fields when computing the Puiseux series above critical points with high algebraic degree over $\mathbb{K}$).

Theorem 1 then follows from Theorem 2 by computing the singular parts of the Puiseux series of the polynomial defining C above all critical points of a suitable projection $C \to \mathbb{P}^1$, and by applying eventually the Riemann-Hurwitz formula. We can derive also from Theorem 2 a quasi-optimal factorization algorithm in $\mathbb{K}[[x]][y]$, which has a special interest with regards to the irreducible decomposition of algebraic plane curves [11].

Theorem 2 leads in particular to an irreducibility test in $\mathbb{K}[[x]][y]$ running with complexity $\tilde{\mathcal{O}}(d\delta)$. If time permits, I will present an algorithm which allows to get rid of the d factor. Keeping hypothesis of Theorem 2, we prove the following result [10,Thm.1]:

Theorem 3. *We can test if F is irreducible in $\mathbb{K}[[x]][y]$ with $\tilde{\mathcal{O}}(\delta + d)$ operations over $\mathbb{K}$ and at most two degree d univariate irreducibility tests over $\mathbb{K}$.*

If F is Weirestrass, the complexity drops to $\tilde{\mathcal{O}}(\delta)$ and one univariate irreducibility test. If F is given as a dense bivariate polynomial in $\mathbb{K}[x, y]$, the complexity is quasi-linear with respect to the arithmetic size of the input. This algorithm is of a different nature than the algorithm of Theorem 2, as we do not use here the usual monomial transforms (blow-ups) and shifts inherent to the Newton-Puiseux type algorithms. We rather generalize Abhyankhar's irreducibility criterion [1] to the case of non algebraically closed residue fields. The main idea is to detect the irreducibility of F on its Ψ-adic expansion, where $\Psi = (\psi_0, \ldots, \psi_k)$ is the collection of some well chosen *approximate roots* of F that we update at each step of the algorithm.

Remark. The three algorithms described above are purely symbolic. They are completely deterministic except for the use of a Las Vegas subroutine for computing primitive elements in the various residue fields extensions, thus avoiding to deal with towers of algebraic extensions of $\mathbb{K}$. However, thanks to the recent preprint [6], we expect that they become deterministic up to substituting d by $d^{1+o(1)}$ in our complexity estimates. Theorem 1 provides a worst-case complexity bound which is equivalent (up to a logarithmic factor) to the computation of the discriminant of a degree d bivariate polynomial, and improving this complexity would be a major breakthrough in Computer Algebra. However, this provides for the moment only a theoretical result : our algorithm is a combination of many subroutines, and the implementation of a fast efficient version would require a huge amount of work, especially due to the dynamic evaluation part. We are currently investigating alternative algorithms based on approximate roots which are easier to implement.

References

[1] S.S. ABHYANKAR, Irreducibility criterion for germs of analytic functions of two complex variables. *Adv. Mathematics* **35**:190–257 (1989).

[2] A. BOSTAN; F. CHYZAK; B. SALVY; G. LECERF; E. SCHOST, Differential equations for algebraic functions. In *Proceedings of ISSAC'07*, 25–32 (2007).

[3] O. Cormier; M.F. Singer; F. Ulmer, Linear differential operators for polynomial equations, *J. of Symb. Comp.*, **34**(5):355–398 (2002).

[4] D. Duval, Rational Puiseux expansions, *Compos. Math.* **70**(2):119–154 (1989).

[5] M. Hodorog; B. Mourrain; J. Schicho, GENOM3CK: a library for genus computation of plane complex algebraic curves using knot theory, in *Comm. in Comp. Alg.*, **44**, ACM (2010).
[6] G. Lecerf; J. Van Der Hoeven, Accelerated tower arithmetic, *Preprint* hal-01788403 (2018).
[7] A. Poteaux; M. Rybowicz, Good reduction of puiseux series and applications, *J. of Symb. Comp.*, **47**(1):32 – 63 (2012).
[8] A. Poteaux; M. Rybowicz, Improving complexity bounds for the computation of puiseux series over finite fields, in *Proceedings of ISSAC'15*, 299–306, ACM (2015).
[9] A. Poteaux; M. Weimann, Computing Puiseux series: a fast divide and conquer algorithm, *Preprint* arXiv:1708.09067v2 (2018).
[10] A. Poteaux; M. Weimann, A quasi-linear irreducibility test in $\mathbb{K}[[x]][y]$, *Preprint* arXiv:1904.00286v1 (2019).
[11] M. Weimann, Bivariate factorization using a critical fiber, *J. Found. of Comp. Math.*, **17**(5):1219–1263 (2016).

S3 - Computational Differential and Difference Algebra and its Applications

Differential transcendence of elliptic hypergeometric functions through Galois theory

Carlos E. Arreche[1] **, *Thomas Dreyfus***[2] **, *Julien Roques***[3] [arreche@utdallas.edu]

[1] Mathematics Department, The University of Texas at Dallas, Richardson, TX, USA
[2] Institut de Recherche Mathématique Avancée, Strasbourg, France
[3] Institut Camille Jordan, Université de Lyon 1, Lyon, France

Elliptic hypergeometric functions arose roughly 10 years ago as a generalization of classical hypergeometric functions and q-hypergeometric functions. These special functions enjoy remarkable symmetry properties, like their more classical counterparts, and find applications in mathematical physics. After interpreting one of these symmetries as a linear difference equation over an elliptic curve, we apply the differential Galois theory of difference equations to show that these functions are always differentially transcendental for “generic" values of the parameters.

Keywords
Elliptic hypergeometric functions, Differential Galois theory

References

[1] C. Arreche, T. Dreyfus, and J. Roques, On the differential transcendence of the elliptic hypergeometric functions. (2018). arXiv:1809.05416.

The generalized Weyl Poisson algebras and their Poisson simplicity criterion

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

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

A new large class of Poisson algebras, the class of *generalized Weyl Poisson algebras*, is introduced. It can be seen as Poisson algebra analogue of the *generalized Weyl algebras* or as giving a Poisson structure to (certain) generalized Weyl algebras. A Poisson simplicity criterion is given for generalized Weyl Poisson algebras and explicit descriptions of the Poisson centre and the absolute Poisson centre are obtained. Many examples are considered.

Keywords
Poisson algebra, a generalized Weyl Poisson algebra, the Poisson centre, the Poisson simplicity.

References

[1] V. V. Bavula, *The generalized Weyl Poisson algebras and their Poisson simplicity criterion*. arXiv:1902.00695.

A computational method for the strong minimality of differential equations

James Freitag[1] [freitagj@gmail.com]

[1] Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago

Over the last several decades a number of significant applications of model theory and differential algebra to number theoretic problems have relied on establishing the strong minimality of the solution set of a differential or difference equation. Strong minimality is a fundamental notion from model theory which is closely related (in the differential setting) to irreducibility in the sense of Painlevé. Usually, the condition is very difficult to establish for nonlinear differential equations of order greater than one. After explaining strong minimality and its importance, we will present a new method for establishing the property which relies on an algorithmic process on linear differential equations and jet spaces.

Keywords
algebraic differential equations, jet spaces, model theory

Order bounds for differential elimination algorithms

Richard Gustavson[1] [rgustavson01@manhattan.edu]

[1] Department of Mathematics, Manhattan College, Riverdale, New York, USA

Differential elimination is the process of eliminating a fixed set of unknown functions from a system of differential equations in order to obtain differential consequences of the system that do not depend on the eliminated functions. The Rosenfeld-Gröbner algorithm, which first appeared in [1], approaches the problem of differential elimination through differential decomposition, that is, by breaking down the original system of differential equations into a collection of simpler systems that can be more easily studied. Properties of these simpler differential systems (for example, whether or not they depend on the to-be-eliminated functions) can then be used to determine information about the original system of differential equations.

In this talk we will discuss the complexity of the Rosenfeld-Gröbner algorithm in terms of the orders of the derivatives that appear in the algorithm. The first such complexity bound was found in [2] for the case of a single derivation. In [3] this was extended to the case of an arbitrary number of derivations. This new upper bound is made possible by associating to the algorithm certain antichain sequences that could be bounded using new results in [4]; the upper bound is then given in terms of the length of these antichain sequences. Also presented is a refined bound for the case of two derivations. The talk is based on joint work with Alexey Ovchinnikov and Gleb Pogudin.

Keywords
Partial Differential Equations, Differential Elimination, Rosenfeld-Gröbner Algorithm

References

[1] F. BOULIER, D. LAZARD, F. OLIVIER, M. PETITOT, Representation for the radical of a finitely generated differential ideal. In *ISSAC '95: Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation*, A.H.M. Levelt (ed.), 158–166. ACM Press, New York, 1995.
[2] O. GOLUBITSKY, M. KONDRATIEVA, M. MORENO MAZA, A. OVCHINNIKOV, A bound for the Rosenfeld-Gröbner algorithm *J. Symb. Comput.* **43**(8), 582–610 (2008).
[3] R. GUSTAVSON, A. OVCHINNIKOV, G. POGUDIN, New order bounds in differential elimination algorithms *J. Symb. Comput.* **85**, 128–147 (2018).
[4] O. LEÓN SÁNCHEZ, A. OVCHINNIKOV, On bounds for the effective differential Nullstellensatz *J. Algebra* **449**, 1–21 (2016).

Hilbert-type Functions of Non-reflexive Prime Difference Polynomial Ideals

Alexander Levin [levin@cua.edu]

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

We introduce a Hilbert-type dimension function associated with a prime non-reflexive difference polynomial ideal and present some conditions under which this function is polynomial. In particular, we give a new proof of the fact that the dimension function is polynomial in the ordinary case and obtain a method of computation of the corresponding dimension polynomial. The existence of such a polynomial was first established in [1, Section 4.4]; an alternative proof was obtained in [5, Section 5.1]. However, these proofs are not constructive, while our approach via the technique of characteristic sets leads to an algorithm for computing dimension polynomials. The following is an overview of the presentation.

Let K be a difference field with a basic set of mutually commuting endomorphisms $\sigma = \{\alpha_1, \dots, \alpha_m\}$ and T the free commutative semigroup generated by σ. If $\tau = \alpha_1^{k_1} \dots \alpha_m^{k_m} \in T$ $(k_1, \dots, k_m \in \mathbf{N})$, then the number $\operatorname{ord} \tau = \sum_{i=1}^{m} k_i$ is called the *order* of τ; if $r \in \mathbb{N}$, we set $T(r) = \{\tau \in T \mid \operatorname{ord} \tau \le r\}$. In what follows we will often use the prefix σ- instead of the adjective "difference".

Let $R = K\{y_1, \dots, y_n\}$ be the ring of difference (σ-) polynomials in n σ-indeterminates over K. (As a ring, $R = K[\{\tau y_i \mid \tau \in T,\ 1 \le i \le n\}]$). By a σ-ideal of R we mean an ideal I of R such that $\alpha_i(I) \subseteq I$ for $i = 1, \dots, m$. A σ-ideal I of R is called *reflexive* if for any $\tau \in T$, the inclusion $\tau(f) \in I$ $(f \in R)$ implies that $f \in I$. For any σ-ideal I of R, the set $I^* = \{f \in R \mid \tau(f) \in I$ for some $\tau \in T$ is the smallest reflexive σ-ideal containing I; it is called the *reflexive closure* of I.

Let P be a prime σ-ideal of R and P^* the reflexive closure of P (it is easy to see that P^* is a prime reflexive σ-ideal of R) and for every $r \in \mathbb{N}$, let $R_r = K[\{\tau y_i \mid \tau \in T(r), 1 \le i \le n\}]$. In other words, R_r is a polynomial ring over K in indeterminates τy_i such that $\operatorname{ord} \tau \le r$. Let $P_r = P \bigcap R_r$, $P_r^* = P^* \bigcap R_r$, and let L, L^*, L_r and L_r^* denote the quotient fields of the integral domains R/P, R/P^*, R_r/P_r and R_r/P_r^*, respectively. If η_i denotes the canonical image of y_i in R_r/P_r^*, then L^* is a σ-field extension of K, $L^* = K\langle \eta_1, \dots, \eta_n \rangle$ (as a field, $L^* = K(\{\tau\eta_i \mid \tau \in T, 1 \le i \le n)\})$ and $L_r^* = K(\{\tau\eta_i \mid \tau \in T(r), 1 \le i \le n\})$. As it is proven in [3] (see also [2, Section 6.4] and [4, Section 4.2]), there exists a polynomial $\phi(t) \in \mathbb{Q}[t]$ such that $\phi(r) = \operatorname{tr.deg}_K K(\{\tau\eta_j \mid \tau \in T(r), 1 \le j \le n\})$ for all sufficiently large $r \in \mathbb{N}$. ($\phi(t)$ is called the *dimension polynomial* of the ideal P^*). However, it is not known in general whether there is a similar polynomial associated with the field extensions L_r/K $(r \in \mathbb{N})$ if $m > 1$. (Since elements of σ do not act on R/P as injective endomorphisms, they do not induce a difference field structure of L. Therefore, one cannot apply the results on filtrations of difference field extensions to the extension L/K.) Using the method of characteristic sets we prove the following results about the function $\psi(r) = \operatorname{tr.deg}_K L_r$.

(i) If $m = 1$, then for all sufficiently large $r \in \mathbb{N}$, $\psi(r) = ar + b$, where $a, b \in \mathbb{Z}$, and $\psi(r) = \phi(r) + c$ where $c \in \mathbb{N}$. (As a consequence, one obtains that in this case the length of an ascending chain of prime difference ideals between P and P^* does not exceed c.)

(ii) If $m > 1$ and every element of a characteristic set of P, written as a polynomial of its leader, has at least one coefficient that does not lie in P^*, then the function $\psi(r)$ is eventually polynomial. In particular, it is the case if the prime difference ideal P is linear or quasi-linear.

We will also discuss some consequences of the obtained results.

This work was supported by the NSF grant CCF-1714425.

Keywords
Difference field, Ring of difference polynomials, Difference ideal, Dimension polynomial, Characteristic set

References
[1] E. HRUSHOVSKI, The Elementary Theory of the Frobenius Automorphisms. *arXiv:math 0406514v1*, 1–135 (2004). Updated version (2012): http://www.ma.huji.ac.il/ ehud/FROB.pdf
[2] M. V. KONDRATEVA; A. B. LEVIN; A. V. MIKHALEV' E. V. PANKRATEV, *Differential and Difference Dimension Polynomials.* Kluwer Academic Publishers, Dordrecht, 1998.
[3] A. B. LEVIN, Characteristic Polynomials of Filtered Difference Modules and Difference Field Extensions. *Russian Math Surv.* **33**, 165–166 (1978).
[4] A. B. LEVIN, *Difference Algebra.* Springer, New York, 2008.
[5] M. WIBMER, Algebraic Difference Equations. Lecture Notes.
`https://www.math.upenn.edu/~wibmer/AlgebraicDifferenceEquations.pdf` (2013).

A Maple package for solving algebraic differential equations by algebro-geometric methods†

Johann J. Mitteramskogler[1] **,**
Wolfgang Schreiner[1] **,** ***Franz Winkler***[1] `[johann.mitteramskogler@risc.jku.at]`

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

AGADE (Algebro-Geometric methods for solving Algebraic Differential Equations) is a software package for computing various types of symbolic solutions for algebraic differential equations (ADEs). This project is still in an early stage of development. We plan to present solution algorithms for finding rational general solutions of first-order (non-linear) ordinary ADEs based on the approaches in Feng and Gao [1, 2] and Ngô and Winkler [3, 4]. The computation of this type of solution, which must contain a transcendental constant, requires knowledge of explicit degree bounds for rational invariant algebraic curves in the case of non-autonomous ADEs. Such a bound is, however, only known in the generic non-dicritical case [5]. An algorithmic way of completely deciding the existence of—and in the positive case, computing—rational general solutions is known for the subclass where the transcendental constant appears rationally [6]. An implementation of the latter method will be part of a subsequent release, however. Later versions of the package will also provide methods for other solution types such as algebraic, radical or formal power series solutions, as well as semi-algorithmic procedures for partial ADEs and systems thereof. An overview can be found in Grasegger and Winkler [7, 8]. All solution methods utilize an approach known as the algebro-geometric method for solving ADEs [9]. A crucial step in this approach is the parametrization of an algebraic variety obtained from the differential equation, where the type of the parametric equations follows from the solution class one is interested in. Given a suitable parametrization of this variety, one obtains an associated system of differential equations whose solution set is in one-to-one correspondence with the solutions of the original ADE. Due to its special form, solutions of the associated system can be computed by well-known methods and are then transformed back to solutions of the original differential equation. This software package is developed for the widely used computer algebra system Maple‡.

Keywords
Algebraic differential equation, rational general solution, symbolic computation, parametrization, software package

References

[1] R. FENG; X. S. GAO, Rational general solutions of algebraic ordinary differential equations. In Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation, 155–162, Santander, Spain, 2004.

†This project is supported by the Austrian Science Fund (FWF): P31327-N32

‡Maple (2018). Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario.

[2] R. FENG; X. S. GAO, A polynomial time algorithm for finding rational general solutions of first order autonomous ODEs. *Journal of Symbolic Computation* **41**(7), 739–762 (2006).
[3] L. X. C. NGÔ; F. WINKLER, Rational general solutions of first order non-autonomous parametrizable ODEs. *Journal of Symbolic Computation* **45**(12), 1426–1441 (2010).
[4] L. X. C. NGÔ; F. WINKLER, Rational general solutions of planar rational systems of autonomous ODEs. *Journal of Symbolic Computation* **46**(10), 1173–1186 (2011).
[5] M. M. CARNICER, The Poincaré problem in the nondicritical case. *Annals of Mathematics* **140**(2), 289–294 (1994).
[6] N. T. VO; G. GRASEGGER; F. WINKLER, Deciding the existence of rational general solutions for first-order algebraic ODEs. *Journal of Symbolic Computation* **87**, 127–139 (2018). [7] G. GRASEGGER; F. WINKLER, *Symbolic solutions of first-order algebraic ODEs.* J. Gutierrez, J. Schicho, M. Weimann (eds.), LNCS volume 8942, 94–104, Springer International Publishing, 2015.
[8] G. GRASEGGER; F. WINKLER, A solution method for autonomous first-order algebraic partial differential equations. *Journal of Computational and Applied Mathematics* **300**, 119–133 (2016).
[9] F. WINKLER, The algebro-geometric method for solving algebraic differential equations — A survey. *Journal of Systems Science and Complexity* **32**(1), 256–270 (2019).

On the Complexity of Computing the Galois Group of a Linear Differential Equation

Mengxiao Sun[1] [msun@gradcenter.cuny.edu]

[1] Department of Mathematics, The Graduate Center, CUNY, New York, NY

The complexity of computing the Galois group of a linear differential equation is of general interest. In a recent work [1], Feng gave the first degree bound on Hrushovski's algorithm [3] for computing the Galois group of a linear differential equation. This bound is the degree bound of the polynomials used in the first step of the algorithm and is quintuply exponential in the order of the differential equation. We use Szántó's algorithm [1], [4] of triangular representation for algebraic sets to analyze the complexity of computing the Galois group of a linear differential equation and we give a new bound which is triple exponential in the order of the given differential equation.

This research has been partially supported by the NSF grants CCF-1563942 and DMS-1760448 and by the PSC-CUNY grant 60098-00 48.

Keywords
Differential Galois groups, linear differential equations, algorithms, triangular sets

References

[1] E. AMZALLAG; G. POGUDIN; M. SUN; N. T. VO, Complexity of triangular representations of algebraic sets. *Journal of Algebra* **523**, 342–364 (2019).
[2] R. FENG, Hrushovski's algorithm for computing the Galois group of a linear differential equation. *Advances in Applied Mathematics* **65**, 1–37 (2015).
[3] E. HRUSHOVSKI, Computing the Galois group of a linear differential equation. *Banach Center Publications* **58**(1), 97–138 (2002).
[4] Á. SZÁNTÓ, Complexity of the Wu-Ritt decomposition. In *Proceedings of the Second International Symposium on Parallel Symbolic Computation*, M. Hitz (eds.), 139–149. ACM, New York, 1997.

A differential algebra approach to parameter identifiability in ODE models

Alexey Ovchinnikov*[2,3]*,
***Gleb Pogudin*[4]*,* *Peter Thompson*[1]** [pthompson@gradcenter.cuny.edu]

[1] CUNY Graduate Center, Ph.D. program in Mathematics, New York,
[2] CUNY Graduate Center, Ph.D. programs in Mathematics and Computer Science, New York
[3] CUNY Queens College, Department of Mathematics, Queens
[4] Courant Institute, New York University, New York

We study structural identifiability of parameterized ordinary differential equation models of physical systems, for example, systems arising in biology and medicine. A parameter is said to be structurally identifiable if its numerical value can be determined from perfect observation of the observable variables in the model. Structural identifiability is necessary for practical identifiability.

The question of parameter identifiability is of great importance in modeling, e.g. in biological systems. Recent work studies identifiability in oncology ([1]), phylogeny ([2]), and cardiovascular models ([3]). Various techniques have been used to study identifiability, and the use of differential algebra in particular extends back 30 years (see, e.g., [4]).

We study structural identifiability via differential algebra. In particular, we use characteristic sets. A system of ODEs can be viewed as a set of differential polynomials in a differential ring, and the consequences of this system form a differential ideal. This differential ideal can be described by a finite set of differential equations called a characteristic set. The technique of studying identifiability via a set of special equations, sometimes called "input-output" equations, has been in use for the past thirty years. However it is still a challenge to provide rigorous justification for some conclusions that have been drawn in published studies.

Our main result is on linear systems. Identifiability in linear systems is a topic of current interest (see [5], [6], [7], [8], [9], [10]). We show that for a linear system of ODEs with one output, the coefficients of a monic characteristic set are identifiable. This refines results presented in [10] and [6]. Our result can be generalized, with additional hypotheses, to nonlinear systems with multiple outputs.

Acknowledgments
This work was partially supported by the NSF grants DMS-1760448, CCF-1563942, DMS-1606334, CCF-0952591, CCF–1708884 and NSA grants #H98230-18-1-0016 and #H98230-15-1-0245.

Keywords
Identifiability, Mathematical Biology

References

[1] A. BROUWER; R. MEZA; M. EISENBERG, A Systematic Approach to Determining the Identifiability of Multistage Carcinogenesis Models. *Risk Analysis* **37**(7), 1375–1387 (2016).
[2] C. DURDEN; S. SULLIVANT, Identifiability of Phylogenetic Parameters from k-mer Data Under the Coalescent. *Bulletin of Mathematical Biology* **81**(2), 431–451 (2019).
[3] A. MAHDI; N. MESHKAT; S. SULLIVANT, Structural Identifiability of Viscoelastic Mechanical Systems. *PLOS ONE* **9**, 1–10 (2014).
[4] E. WALTER AND L. PRONZATO, On the identifiability and distinguishability of nonlinear parametric models. *Mathematics and Computers in Simulation* **42**(2), 125–134 (1996).
[5] N. MESHKAT; S. SULLIVANT, Identifiable reparametrizations of linear compartment models. *Journal of Symbolic Computation* **63**, 46–67 (2014).
[6] N. MESHKAT; S. SULLIVANT; M. EISENBERG, Identifiability Results for Several Classes of Linear Compartment Models. *Bulletin of Mathematical Biology* **77**, 1620–1651 (2014).
[7] E. GROSS; N. MESHKAT; A. SHIU, Identifiability of linear compartment models: the singular locus. (submitted September, 2017). [8] J. BAAIJENS; J. DRAISMA, On the Existence of Identifiable Reparametrizations for Linear Compartment Models. *SIAM Journal on Applied Mathematics* **76**(4), 1577–1605 (2016).
[9] J. YATES; N. EVANS; M. CHAPPELL, Structural identifiability analysis via symmetries of differential equations. *Automatica* **45**(11), 2585–2591 (2009).
[10] E. GROSS; H. HARRINGTON; N. MESHKAT; A. SHIU, Linear compartment models: input-output equations and operations that preserve identifiability. (submitted 2019).

S4 - Computer Algebra and Application to Combinatorics, Coding Theory and Cryptography

Distributed Coded Computation

Malihe Aliasgari[1] [ma839@njit.edu]

[1] Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ, U.S.A.

The era of Big Data and the immensity of real-life datasets compels computation tasks to be performed in a distributed fashion, where the data is dispersed among many servers that operate in parallel. However, massive parallelization leads to computational bottlenecks due to faulty servers and stragglers. Stragglers refer to a few slow or delay-prone processors that can bottleneck the entire computation because one has to wait for all the parallel nodes to finish. The problem of straggling processors, has been well studied in the context of distributed computing e.g., [1], [2]. Recently, it has been pointed out that, for the important case of linear functions, it is possible to improve over repetition strategies in terms of the tradeoff between performance and latency by carrying out linear precoding of the data prior to processing, e.g., [3], [4]. The key idea is that, by employing suitable linear codes operating over fractions of the original data, a function may be completed as soon as enough number of processors, depending on the minimum distance of the code, have completed their operations.

Coding has also been found to be useful addressing the straggler problem in the context of coded distributed storage and computing systems. Coded computation which is a topic of active interest with several interesting works, also provides novel analyses of required computation time (e.g. expected time or decoding latency). The implementation of coded computation over the multiple processors is faced not only with the challenge of providing reliable operation despite the unreliability of the processors, but also with the latency constraints imposed by retransmission protocols. In particular, keeping decoding latency at a minimum is a major challenge. In [1], [2] it is argued that exploiting parallelism across multiple cores in the distributed system can reduce the decoding latency by enabling decoding as soon as one can has computed its task.

The problem of matrix-matrix multiplication in the presence of practically big sized of data sets faced with computational and memory related difficulties, which makes such operations are carried out using distributed computing platforms [5], [6]. In this work, we study the problem of distributed matrix-matrix multiplication $\mathbf{W} = \mathbf{XY}$ under storage constraints, i.e., when each server is allowed to store a fixed fraction of each of the matrices $\mathbf{X}$ and $\mathbf{Y}$, which is a fundamental building of many science and engineering fields such as machine learning, image and signal processing, wireless communication, optimization. Although distributed matrix-matrix multiplication can resolve computational and memory related difficulties, it causes new security problems. One may want to do some computing on some private information. We consider the problem of computing the matrix multiplication $\mathbf{W} = \mathbf{XY}$ in a distributed computing system of multiple workers which process each worker only a fraction of the input matrices. Three performance criteria are of interest:

- the recovery threshold, that is, the number of workers that need to complete their task before the master server can recover the product $\mathbf{W}$;
- the communication load between workers and master server;
- the tolerated number of colluding servers that ensures perfect secrecy for both data matrices $\mathbf{X}$ and $\mathbf{Y}$.

Keywords
Coded distributed computation, Linear code, Secret sharing, Stragglers

References

[1] S. LI; M. A. MADDAH-ALI; Q. YU; A. S. AVESTIMEHR, A fundamental tradeoff between computation and communication in distributed computing. *IEEE Transactions on Information Theory*, **65**(1), 109–128 (2018).
[2] M. ALIASGARI; J. KLIEWER; O. SIMEONE, Coded computation against processing delays for virtualized cloud-based channel decoding. *IEEE Transaction on Communication* **67**(1), 28–38 (2019).
[3] S. DUTTA; V. CADAMBE; P. GROVER, Short-Dot: Computing large linear transforms distributedly using coded Short-Dot products. *in Advances In Neural Information Processing Systems (NIPS)*, 2092–2100. 2016.
[4] M. ALIASGARI; J. KLIEWER; O. SIMEONE, Coded computation against straggling decoders for network function virtualization. *in Processing IEEE International Symposium Information Theory (ISIT)* 711–715. USA, Vail, 2018.
[5] M. FAHIM; H. JEONG; F. HADDADPOUR; S. DUTTA; V. CADAMBE; P. GROVER, On the optimal recovery threshold of coded matrix multiplication. *in Communication, Control, and Computing (Allerton)* 1264–1270. USA. 2017.
[6] M. ALIASGARI; O. SIMEONE; J. KLIEWER, Distributed and private coded matrix computation with flexible communication load. *arXiv preprint, arXiv:1901.07705v1*, 2019.

Searching for projective planes with computer algebra and SAT solvers

Curtis Bright[1], *Kevin Cheung*[2], *Vijay Ganesh*[1],
Ilias Kotsireas[3], *Dominique Roy*[4], *Brett Stevens*[2] [cbright@uwaterloo.ca]

[1] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada
[2] School of Mathematics and Statistics, Carleton University, Ottawa, Canada
[3] Department of Physics and Computer Science, Wilfrid Laurier University, Waterloo, Canada
[4] Canada Revenue Agency, Ottawa, Canada

In the 1970s and 1980s a series of exhaustive searches [1–4] showed that projective planes of order ten do not exist. These searches required a significant amount of computing power including almost three months of time on a CRAY-1A supercomputer. However, due to the nature of the search it was not possible to present a formal proof of the result. Recently SAT solvers have been used to derive proofs of results that require extensive computer search [5], raising the possibility that SAT solvers could be useful searching for projective planes and proving that projective planes of certain orders do not exist.

In this talk we report on work we have done in this direction, in particular, employing a hybrid satisfiability checking and computer algebra (SAT+CAS) approach that has been recently proposed [6] and successfully used in searches for other combinatorial objects [7–9]. In the SAT+CAS paradigm a computer algebra system is used to generate theory lemmas that a SAT solver would otherwise not be able to learn. In the search for projective planes we found that a CAS is an effective tool for finding symmetries of partial projective planes that can be used to dramatically improve the efficiency of the SAT solver.

Keywords
Projective planes, satisfiability checking, symbolic computation, symmetry breaking, search

References

[1] F. J. MacWilliams; N. J. A. Sloane; J. G. Thompson, On the existence of a projective plane of order 10. *Journal of Combinatorial Theory, Series A*, **14**(1), 66–78 (1973).
[2] J. L. Carter, *On the existence of a projective plane of order ten.* PhD thesis, University of California, Berkeley, 1974.
[3] C. W. H. Lam; L. Thiel; S. Swiercz, The nonexistence of code words of weight 16 in a projective plane of order 10. *Journal of Combinatorial Theory, Series A*, **42**(2), 207–214 (1986).
[4] C. W. H. Lam; L. Thiel; S. Swiercz, The non-existence of finite projective planes of order 10. *Canadian Journal of Mathematics*, **41**(6), 1117–1123 (1989).
[5] M. J. H. Heule; O. Kullmann; V. W. Marek, Solving and verifying the boolean Pythagorean triples problem via cube-and-conquer. In *Theory and Applications of Satisfiability Testing – SAT 2016*, N. Creignou and D. Le Berre (eds.), 228–245. Springer, Cham, 2016.

[6] E. ÁBRAHÁM, Building bridges between symbolic computation and satisfiability checking. In *ISSAC'15 Proceedings of the 2015 ACM International Symposium on Symbolic and Algebraic Computation*, S. Linton (ed.), 1–6. ACM, New York, 2015.
[7] C. BRIGHT; I. KOTSIREAS; V. GANESH, Applying computer algebra systems with SAT solvers to the Williamson conjecture. *Journal of Symbolic Computation*, to appear (2019).
[8] C. BRIGHT; I. KOTSIREAS; A. HEINLE; V. GANESH, Enumeration of complex Golay pairs via Programmatic SAT. In *ISSAC '18 Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation*, C. Arreche (ed.), 111–118. ACM, New York, 2018.
[9] C. BRIGHT; D. Ž. ĐOKOVIC; I. KOTSIREAS; V. GANESH, A SAT+CAS approach to finding good matrices: New examples and counterexamples. To appear in *Proceedings of the Thirty-Third AAAI Conference on Artificial Intelligence*, AAAI Press, Palo Alto, 2019.

Code-based cryptography : from McEliece to the NIST competition

Pierre-Louis Cayrel[1] [pierre.louis.cayrel@univ-st-etienne.fr]

[1] Laboratoire Hubert Curien, Université de Lyon, Saint-Etienne, France

A lot of research has been done on quantum computers in recent years. Those are computers that exploit the properties of quantum mechanics for solving mathematical problems difficult to solve for classical computers (the factorization of integers and the problem of discrete logarithms, for instance). If large-scale quantum computers are built, they will be able to break most public key cryptosystems currently used in communication systems such as RSA or ECC. So the cryptographic community has turned to creative alternatives to dealing with quantum computing. The first quantum resistant public key cryptosystem dates back to 1978 with McEliece PKC [1]. In November 2017, 82 applications were submitted to NIST [2]. On January 30th 2019, 26 candidates were chosen for the second round of NIST. This election was based on evaluation criteria, reactions of the cryptographic community and internal reviews of the candidates. In order of importance we first have safety, then cost and performance and finally the implementation characteristics of the algorithm. To assess the security of an algorithm, NIST first examines the security arguments presented in the submission, as well as external cryptanalysis. Next, NIST researchers also perform an internal cryptanalysis of the submission. NIST considers not only attacks that directly demonstrate that a candidate is not really secure, but also attacks that undermine the candidate's underlying security concerns or give rise to potential threats. NIST also examines the quantity, quality, and maturity of the overall analysis for each candidate, including the analysis of similar schemes. After security, the most important criterion for choosing the second round is performance. NIST takes into account both the computational efficiency for key generation, the memory used, the size of the public key, the size of the ciphertext, the probability of decoding failure and the speed of execution of the algorithm. We will briefly present the 7 code-based candidates who passed the second round and detail insights on research perspectives of the next years.

Keywords
Code-based cryptography, McEliece encryption scheme, NIST PQ cryptography competition

References

[1] R. McEliece, *A public-key cryptosystem based on algebraic coding theory*. DSN Prog. Rep., Jet Prop. Lab., California Inst. Technol., Pasadena, CA, pages 114 116, Jan. 1978.
[2] NIST, *https://csrc.nist.gov/Projects/Post-Quantum-Cryptography*.

HELP: the knight gambit for efficient decoding of BCH codes

Michela Ceria[1] ***, Teo Mora***[2] ***, Massimiliano Sala***[3] [michela.ceria@unimi.it]

[1] Department of Computer Science, Università degli Studi di Milano, Italy
[2] Department of Mathematics, University of Genoa, Italy
[3] Department of Mathematics, University of Trento, Italy

In the context of Cooper Phylosophy [3, 4], which suggested to use Groebner bases to decode cyclic codes, very important concepts are those of *syndrome ideal* and *syndrome variety*. The syndrome variety is a finite set of points, whose components are syndromes and the corresponding error locations, while the *syndrome ideal* is the vanishing ideal of the syndrome variety.
Sala and Orsini [5] defined a new syndrome variety which removes the so called *spurious solutions*, namely points not corresponding to any error vector. They also introduced the so called *general error locator polynomial* (GELP), a polynomial $\sigma(z,s)$ such that, if the error correction capability of the considered cyclic code is t and $\mu \le t$ errors occurred, then, given the corresponding syndrome vector $\overline{s}$, the roots of $\sigma(z,\overline{s})$ are the μ error locations and zero with multiplicity $t-\mu$. Moreover, they proved that every cyclic code admits a GELP.
Since the bottleneck in the decoding procedure, using such a polynomial, is the evaluation in the syndrome vector, it is useful to find a *sparse* version of such a polynomial and our analysis started from this point.
In the case $t \le 2$, using Marinari-Mora Axis of Evil Theorem [1, 2], and studying the very particular structure of the lexicographical Groebner escalier of the syndrome ideal, it is possible to linearly deduce one error location from the other. Therefore, it is not necessary to compute both the roots of $\sigma(s,z)$ at a syndrome vector, but only one is enough. This implies that we can define the *half error locator polynomial* (HELP), which is linear in z and provides anyway all the needed information. In principle, such a polynomial should be computed by interpolating half of the points in the syndrome variety, the other being desumed by the linear relation.
Working on the HELP by inspection, we found out that all the (narrow-sense primitive) BCH codes over $GF(2^m)$ have sparse half error locator polynomials, obeying to the same pattern. They have at most $\frac{n+1}{2}+1$ terms with nonzero coefficients, where $n = 2^m-1$ and the polynomials have the following shape, where each monomial $x_1^{(4-3i) \mod n} x_2^{(i-1) \mod \frac{n+1}{2}}$ is obtained from the previous one, by performing a knight $(-3,1)$ move on a $\frac{n+1}{2} \times n$ chess board (whose rows and columns are indexed with the pure powers of the variables x_1, x_2):

$$\sigma(z,x) = z + \sum_{i=1}^{\frac{n+1}{2}} a_i x_1^{(4-3i) \mod n} x_2^{(i-1) \mod \frac{n+1}{2}}, \ x = (x_1, x_2)$$

where $a_i \in GF(2^m)$ are the coefficients.
The next step is the determination of the coefficients $a_i \in GF(2^m)$.

Basing on the information we had by the inspection and using again the Axis of Evil Theorem, we verified that the HELP could be found by Lagrange interpolation on all points of the syndrome variety whose first coordinate is 1:

$$\sigma(z,x) = x_1 g(t)$$

where $g(t)$ is the Lagrange interpolator and $t = x_1^{-3 \mod n} x_2$.
Example For the primitive narrow-sense BCH code over $GF(8)$ we have the polynomial $\sigma(z,x) = z + a^6 x_1^2 x_2^2 + a^4 x_1^5 x_2 + a^3 x_1$. The chess board is

$$\begin{array}{ccccc}
x_1^6 & 0 & 0 & 0 & 0 \\
x_1^5 & 0 & a^4 & 0 & 0 \\
x_1^4 & 0 & 0 & 0 & 0 \\
x_1^3 & 0 & 0 & 0 & 0 \\
x_1^2 & 0 & 0 & a^6 & 0 \\
x_1 & a^3 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
 & 1 & x_2 & x_2^2 & x_2^3
\end{array}$$

Now, considering $t = x_1^4 x_2$, $\sigma(z,x) = z + x_1 g(t)$, where $g(t) = a^6 t^2 + a^4 t + a^3$.

The same approach, with the knight move, allowed to study all cases mentioned in [3].

Keywords
Error locator polynomial, syndrome variety, BCH codes

References

[1] M.E. Alonso, M.G. Marinari, T. Mora, The big Mother of all Dualities 2: Macaulay Bases, Applicable Algebra in Engineering, Communication and Computing archive Vol. 17, Issue 6, November 2006, 409–451.
[2] Ceria, M., A proof of the "Axis of Evil theorem" for distinct points, Rendiconti del Seminario Matematico dell'Università e del Politecnico di Torino, Vol. 72 No. 3-4, pp. 213-233 (2014)
[3] A.B. III Cooper, Direct solution of BCH decoding equations, Comm., Cont. and Sign. Proc. (1990), 281–286.
[4] A.B. III Cooper, Finding BCH error locator polynomials in one step, Electronic Letters 27 (1991), no. 22, 2090–2091.
[5] E. Orsini and M. Sala, General error locator polynomials for binary cyclic codes with $t \leq 2$ and $n < 63$, IEEE Trans. on Inf. Th. 53 (2007), 1095–1107.

Constructions of quantum codes

Reza Dastbasteh[1] **, *Petr Lisoněk***[1] [rdastbas@sfu.ca]

[1] Department of Mathematics, Simon Fraser University, Burnaby, Canada

We review methods for constructing quantum codes from classical additive and linear codes that are self-orthogonal with respect to the symplectic inner product on the ambient vector space. We generalize these constructions to codes that are nearly self-orthogonal. The families of codes considered include additive cyclic codes, twisted codes, and linear cyclic codes. We review the known techniques for bounding the minimum distance of cyclic codes and we show new applications of these techniques to twisted codes. We illustrate the applicability of our methods by presenting many new examples of binary quantum codes that have higher minimum distance than the previously known codes.

Keywords
Quantum stablizer codes, Twisted codes, Minimum distance bounds

Relative projective group ring codes over chain rings

Simon Eisenbarth[1] [simon.eisenbarth@rwth-aachen.de]

[1] Lehrstuhl D für Mathematik, RWTH Aachen, Germany

Let $\mathbb{F}$ be a finite field and let G be a finite group. A (two-sided) ideal in the group ring $\mathbb{F}G$ is called group code. They were introduced by Berman in 1967, who studied cyclic codes as ideals in $\mathbb{F}C_n$ and showed that the Reed-Muller codes are certain powers of the Jacobson-radical in $\mathbb{F}C_2^m$. Later, other well-known linear codes were constructed as ideals in certain group rings. Of particular interest are those codes, which can be realized (up to isomorphism) as group codes over abelian groups. It has been shown, that all group codes of dimension ≤ 3 are abelian group codes ([1]) as well as all codes over a group G admitting a decomposition $G = AB$ in abelian subgroups A and B ([2]). Using the O'Nan-Scott theorem of the maximal subgroups of the symmetric group S_n, we show that almost every group code over the simple group A_5 is non-abelian, except the trivial ones.
Group codes, which are generated by an idempotent, are called projective (of course, if the order of G and the chraracteristic of $\mathbb{F}$ are coprime, every group code is projective by the theorem of Maschke). For an artinian, commutative chain ring R, we extend this definition to relativ-projective group codes in RG, i.e. those codes, which are relative projective for the subgroup $\{1\}$ of G in the sense of homological algebra. We show that all such codes can be constructed with certain idempotents in RG, moreover, they are in bijection with chains of projective group ring codes over $\mathbb{F}G$, where $\mathbb{F}$ is the residue field of R. Most of the properties of a relative projective group code can be derived from such a chain, for example the Hamming distance, the dual code or a lower bound of the euclidian distance.

Keywords
group codes, chain rings, relative projective

References

[1] C. García Pillado, S. González, V. Markov, O. Markova and C. Martínez, Group codes of dimension 2 and 3 are abelian. *Finite Fields and Their Applications* **55**, 167–176 (2019).
[2] José Joaquín Bernal, Ángel del Río and Juan Jacobo Simón, An intrinsical description of group codes. *Des. Codes Cryptogr.* **51(3)**, 289–300 (2009).

Error correcting codes over rings

Kenza Guenda[1]**, *T. Aaron Gulliver*** [1] [kguenda@gmail.com]

[1] Department of Electrical and Computer Engineering, University of Victoria

Error correcting codes play a fundamental role in the field of information theory. Codes over rings are a special class of error correcting codes. These codes have found numerous applications in digital communications. A novel application of codes over rings is in the area of DNA computing. This is a recent application of biology, ring theory and information theory which improves on conventional techniques in computation. There is also interest in the application of codes over rings in the construction of quantum error correcting codes. Recently, the Calderbank, Shor and Steane (CSS) construction has been extended to codes over rings. This produced numerous optimal codes considering the homogeneous weight. The purpose of this talk is to present recent applications of codes over rings in the context of DNA computing, DNA modeling as well as in the area of quantum information.

Keywords
Error correcting codes, Codes over rings, DNA computing, Quantum codes, CSS construction.

References
[1] K. Guenda, T.A. Gulliver, *Construction of cyclic codes over $F_2 + uF_2$ for DNA computing*, Applic. Algebra in Eng. Commun. Computing 24(6), 445–459, 2012. [2] N. Bennenni, K. Guenda, T.A. Gulliver, *Construction of codes for DNA computing by the greedy algorithm*, ACM Commun. Computer Algebra 49(1), 14, 2015. [3]K. Guenda, T.A. Gulliver, *Quantum codes over rings*, Intern. J. Quantum Inform. 12(4), 2014.

Rudin-Shapiro-like sequences with low correlation

Daniel J. Katz[1] [daniel.katz@csun.edu]

[1] Department of Mathematics, California State University, Northridge, USA

The Rudin-Shapiro-like sequences are a family of binary sequences arising from an elegant recursive construction that gives them interesting analytic and combinatorial properties. Borwein and Mossinghoff [1] showed that they also have low mean square aperiodic autocorrelation. This makes them of interest in communications and remote sensing. We give a survey of some recent investigations into the correlation properties of Rudin-Shapiro-like sequences and their relatives, including their crosscorrelation, an important design parameter for multiuser communications networks. The study of these sequences has been aided significantly by computational studies enabled by the use of discrete Fourier analysis, group theory, and large-scale distributed computing.

Keywords
Rudin-Shapiro sequence, correlation, Fourier analysis

References

[1] P. BOWEINN, M. MOSSINGHOFF, Rudin-Shapiro-like polynomials in L_4. *Math. Comp.* **69(231), 1157–1166 (2000).**

Why you cannot even hope to use Gröbner bases in cryptography: an eternal golden braid of failures

***Boo Barkee, Michela Ceria*[1] *, Theo Moriarty*[2] *, Andrea Visconti*[1]** [5919@unige.it]

[1] Department of Computer Science, University of Milan, Italy
[2] Department of Mathematics, University of Genoa, Italy

In 1994, Moss Sweedler's dog [3] proposed a cryptosystem, known as *Barkee's Cryptosystem*, and the related cryptanalysis, with the explicit aim to dispel the proposal of using "the fact that Gröbner bases are hard to compute, to devise a public key cryptography scheme" claiming that "no scheme using Gröbner bases will ever work". Barkee's scheme writes down an easy-to-produce Gröbner basis $F = \{f_1,\ldots,f_s\}$ via Macaulay's Trick [20] generating an ideal $\mathsf{I} := \mathbb{I}(F) \subset \mathscr{P} := k[X_1,\ldots,X_n]$ and publishes a set $G := \{g_1,\ldots,g_l\} \subset \mathbb{I}(F)$ of *dense* polynomials of degree at most d in $\mathscr{P}$ and a set $T := \{\tau_1,\ldots,\tau_s\} \subset \mathbf{N}(\mathbb{I}(F)) = \mathscr{T} \setminus \mathbf{T}(\mathbb{I}(F))$ of *normal terms* "*either the whole of it, or, for added security, a subset of it*" [3] belonging to the Gröbner *éscalier* of $\mathbb{I}(F)$. In order to send a message $M := \sum_{i=1}^{s} c_i\tau_i \in \mathrm{Span}_k(T)$, the sender produces random *dense* polynomials $p_j \in \mathscr{P}, 1 \le j \le l, \deg(p_i) = r$, and encryps M as $C := M + \sum_{j=1}^{l} p_j g_j$; the receiver, possessing the Gröbner basis of $\mathbb{I}(F)$ applies Buchberger's reduction to obtain the canonical form of C: $\mathrm{Can}(C,\mathbb{I}(F)) = M = \sum_{i=1}^{s} c_i\tau_i$.

It is easy to realize that denoting, for each $\delta \in \mathbb{N}$, $\mathscr{T}(\delta) := \{\tau \in \mathscr{T} : \deg(\tau) \le \delta\}$ & $\mathsf{T}(\delta) := \#\mathscr{T}(\delta) = \binom{\delta+n}{n}$ both encoding and decoding costs between $\mathscr{O}(\mathsf{T}(d+r))$ (the time needed to scan a dense message) and $\mathscr{O}(\mathsf{T}^2(d+r))$ (the cost of Buchberger's reduction algorithm in the generic case).

The point of [3] was that an enemy would have been able to read the message without even attempting to perform the hard Gröbner basis computation but with a more elementary linear-algebra based approach. Namely the authors proposed two attacks, one based on [10], with complexity $\mathscr{O}(\mathsf{T}^4(d+r))$, the other solving a *dense* linear algebra problem costing $\mathscr{O}(\mathsf{T}^{2.4\cdots}(d+r))$; later K.W.Lenstra, Jr. proposed a stronger version ([17],pg. 114].†

† B. Barkee *et al.* concluded their paper [3] with a challenge:
"A cryptographic scheme applying the complexity of Gröbner bases to an ideal membership problem is bound to fail. Is our reader able to find a scheme which overcomes this difficulty? In particular our reader could think (perhaps with some reason) that a sparse *scheme could work. We believe (perhaps without reason) that sparsity will make the scheme easier to crack. We would be glad to test our belief on specific sparse schemes."*

Boo was unaware that a *sparse* cryptographic scheme based on the ideal membership problem was already (1992) developed by Fellows and Kobitz [13-15] under the label of *Polly Cracker* where the trapdoor of their system is not a Gröbner basis of the ideal, but, more simply, a root of it. What is more important, the polynomials generating the public ideal are derived from combinatorial or algebraic NP-complete problems (hence such systems were naturally named CA-systems) . This oriented to consider both analysis based on satisfability [18] and attacks exploiting the sparsity of the generators [16,12]. Soon the research oriented toward cryptosystems based on binomail ideals/Euclidean lattices [8]. But this is another story to which Boo did not contribute. For a survey on CA-systems and their analysis see [19].

In 2006, [1] proposed essentially a *verbatim* adaptation of [3]; the main differences are that the Gröbner basis F is taken in a free module over a monoid ring and the public data are the free monoid, the set G (usually a generating set formed by binomials) and the *whole set* $\mathbf{N}(\mathbb{I}(F))$, so that the system is widely open to a oracle attack [5,2].

However, ten years before, Pritchard [24] published a procedure which is able to crack also the obvious improvement of publishing a subset of terms [6]: the existence, in the non-commutative setting, of infinite Gröbner bases implies that Buchberger Algorithm becomes a semidecision procedure which terminates returning a finite Gröbner basis if and only if such basis is finite; Pritchard adapted such version of Buchberger Algoritm into a semidecision procedure which, given a basis $G \subset \mathcal{Q} = k\langle X_1,\dots,X_n\rangle$ and a polynomial $f \in \mathcal{Q}$ terminates if and only if $f \in \mathbb{I}(G)$. It is then a trivial excercise ([21] Figure 47.7) to adapt Pritchard's Procedure in order to produce an *algorithm* to decrypt any non-commutative version of Barkee's Cryptosystem.

Rai's cryptosystem [25], based on the infiniteness of non-commutative Gröbner bases, and consisting in hiding the (principal) Gröbner basis $\{g\}$ into a public basis $\{l_1 g r_1 \dots l_s g r_s\}$ cannot be cracked via Pritchard's algorithms but yields under Davenport's algorithm factorizing non-commutative polynomials [9].

A factorization algorithm [11] broke a Diffie-Hellman scheme on graded Ore extensions [4]; [7] has proposed an improved version on multivariate Ore extensions which can be translated into (graded) *iterated Ore extensions with power substitutions* $\mathscr{A}$ [23,22]: given public 3 non-commuting elements $L, C, R \in \mathscr{A}$, Alice selects two polynomials $l, r \in k[X]$ and sends to Bob $l(L)Cr(R)$. While we do not have techniques for investigating the strength of [7], we guess that our Gröbner oriented extension to [23,22] could be broken both by using Kandri-Rody–Weispfenning result ([21] Prop. 49.3.5) and by an attack through non-commutative one-sided tag-variable tecniques [26], available via Heyworth notation [27].

Keywords
Barkee's Cryptosystem, Polly Cracker, Gröbner bases, Multivariate Ore Extensions

References
[1] Ackermann P., Kreuzer M., *Gröbner Basis Cyptosystems.* J. AAECC **17** (2006).
[2] Alonso M.E., Marinari M.G., Mora T. *Oracle-Supported Drawing of the Gröbner éscalier.* preprint arXiv:1006.3297 [math.AC] (2008).
[3] Barkee B., Can D.C., Ecks J., Moriarty T.,Ree R.F., *Why You Cannot Even Hope to Use Gröbner Bases in Public Key Cryptography.* J. Symb. Comp. **18** (1994), pp. 497–501.
[4] Boucher D., Gaborit P., Geiselmann W., Ruatta O., Ulmer F.. *Key exchange and encryption schemes based on non-commutative skew polynomials.* L.N.C.S. **6061** 126–141. Springer, 2010.
[5] Bulygin S., *Chosen-Ciphertext Attack on Noncommutative Polly Cracker.* preprint available at `http://arxiv.org/abs/cs/0508015v2` (2005).
[6] Bulygin S.V., Rai T.S., *"Countering Chosen-Ciphertext Attacks against Noncommutative Polly Cracker Cryptosystems".* Talk at Special Semester on Gröbner Bases, Linz, May 2006.

[7] Burger, Reinhold, and Albert Heinle. *A Diffie-Hellman-like key exchange protocol based on multivariate Ore polynomials.* preprint (2014).
[8] Massimo Caboara, Fabrizio Caruso, Carlo Traverso *Lattice Polly Cracker cryptosystems.* J. Symb. Comput. 46(5): 534-549 (2011) J. Symb. Comp. **46** (2011)), pp. 534-549.
[9] F. Caruso *Factorization of Non-Commutative Polynomials*
`https://arxiv.org/abs/1002.3180` (2010)
[10] Dickenstein A., Fitchas N., Giusti M., Sessa C., *The Membership Problem* ... Discrete Applied Mathematics **33** (1991), pp. 73–94.
[11] Dubois, Vivien, and Jean-Gabriel Kammerer. *Cryptanalysis of cryptosystems based on non-commutative skew polynomials.* International Workshop on PKC2011. Springer, 2011.
[12] Endsuleit R., Geiselmann W., Steinwandt R., *Attacking a Polynomial-Based Cryptosystem: Polly Cracker.* Int. J. Inf. Secur. **1** (2002), pp. 143–148.
[13] Fellows M.R., Koblitz N., *Kid Krypto.* L.N.C.S. **740** (1993), pp. 371–389.
[14] Fellows M.R., Koblitz N., *Combinatorially Based Cryptography for Children (and Adults).* Congressus Numerantium **99** (1994), pp. 9–41.
[15] Fellows M.R., Koblitz N., *Combinatorial Cryptosystems Galore!".* Contemporary Math. **168** (1994), pp. 51–61.
[16] D. Hofheinz, R. Steinwandt *A "Differential" Attack on Polly Cracker.* Int. J. Inf. Secur. **1** (2002) 143–148.
[17] Koblitz N., *Algebraic Aspects of Cryptography.* Algorithms and Computation in Mathematics , Vol. 3, Springer (1998)
[18] F. Levy-dit-Vehel, L. Perret *A Polly Cracker System Based on Satisfiability* Progress in Computer Science and Applied Logic **23** (2004) 177–192
[19] F. Levy-dit-Vehel, M.G. Marinari, L. Perret, C. Traverso, *A Survey on Polly Cracker Systems* in M. Sala et al. (Ed.) *Gröbner bases, Coding, Cryptography*, Springer Risc XVI, (2009) 285–305
[20] F. Mora. *De Nugis Groebnerialium 2: Applying Macaulay's Trick in order to easily write a Groebner basis* **13** *Journal AAECC* (2003), pp. 437–446.
[21] Mora T., *Solving Polynomial Equation Systems* 4 Vols., Cambridge University Press, I (2003), II (2005), III (2015), IV (2016).
[22] B. Nguefack, E. Pola, *Effective Buchberger-Zacharias-Weispfenning theory of skew polynomial extensions of restricted bilateral coherent rings*, J. Symb. Comp. (2019), Doi:https://doi.org.10.1016/j.jsc.2019.03.003
[23] Pesch M., *Gröbner Bases in Skew Polynomial Rings* Dissertation,Passau (1997)
[24] Pritchard F. L., *The Ideal Membership Problem in Non-Commutative Polynomial Rings.* J. Symb. Comp. **22** (1996), pp. 27–48.
[25] T.S. Rai *Infinite Gröbner bases and Noncommutative Polly Cracker Cryptosystems* PhD Thesis, Virginia Polytechnique Institute and State Univ. (2004)
[26] Shannon, D., Sweedler, M. *Using Gröbner bases to determine algebra membership, splitting surjective algebra homomorphisls and determine birational equivalence* J. Symb. Comp. **6** (1988), 267–273
[27] Heyworth A. *One-sided noncommutative Gröbner bases with Applications to Computing Green's Relations*, J. Algebra **242** (2001) 401-416

Skew constacyclic codes over a non-chain ring $\mathbb{F}_q[u,v]/\langle f(u), g(v), uv-vu\rangle$

***Swati Bhardwaj*[1], *Madhu Raka*[1]** [mraka@pu.ac.in]

[1] Centre for Advanced Study in Mathematics, Panjab University, Chandigarh-160014, INDIA

In 2007, Boucher et al. [1] generalized the concept of cyclic codes over a non-commutative ring, namely skew polynomial ring $\mathbb{F}_q[x;\theta]$, where $\mathbb{F}_q$ is a field with q elements and θ is an automorphism of $\mathbb{F}_q$. Several authors investigated structural properties of skew cyclic codes over fields. Then the attention moved to skew cyclic codes over rings. Many people considered non-chain rings such as $\mathbb{F}_p + v\mathbb{F}_p$, where $v^2 = 1$; $\mathbb{F}_q + v\mathbb{F}_q$, where $v^2 = v$; $\mathbb{F}_q + v\mathbb{F}_q + \cdots + v^{m-1}\mathbb{F}_q$, where $v^m = v$, and studied skew cyclic codes over these, see for example [2], [4], [7], [8]. Recently people have started studying skew cyclic codes over finite non-chain rings having 2 or more variables such as $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, where $u^2 = u, v^2 = v, uv = vu$ or $\mathbb{F}_{p^m}[v,w]/ < v^2-1, w^2-1, vw-wv >$ and also discussed skew constacyclic codes over these, see [5], [6], [9] etc. Also see [3].

In this paper, we study skew cyclic and skew constacyclic codes over a more general ring. Let $f(u)$ and $g(v)$ be two polynomials of degree k and ℓ, not both linear, which split into distinct linear factors over $\mathbb{F}_q$. Let $\mathscr{R} = \mathbb{F}_q[u,v]/\langle f(u), g(v), uv-vu\rangle$ be a finite non-chain ring. A Gray map is defined from $\mathscr{R}^n \to \mathbb{F}_q^{k\ell n}$ which preserves duality. We define two automorphisms ψ and θ_t on $\mathscr{R}$ and discuss ψ-skew cyclic and θ_t-skew α-constacyclic codes over this ring, where α is any unit in $\mathscr{R}$ fixed by the automorphism θ_t, in particular when $\alpha^2 = 1$. Some structural properties, specially generator polynomials and idempotent generators for skew constacyclic codes are determined. Some examples are also given to illustrate the theory.

Keywords
Skew cyclic codes, skew quasi-cyclic codes, quasi-twisted codes, Gray map

References

[1] D. Boucher, W. Geiselmann and F. Ulmer, Skew cyclic codes. *Appl. Algebra Engrg. Comm. Comput.* **18** (4), 379-389 (2007).
[2] J. Gao, F. Ma and F. Fu, Skew constacyclic codes over the ring $\mathbb{F}_q + v\mathbb{F}_q$, *Appl. Comput. Math.* **6**(3), 286-295 (2017).
[3] M. Goyal and M. Raka, Polyadic cyclic codes over a non-chain ring $\mathbb{F}_q[u,v]/\langle f(u), g(v), uv-vu\rangle$, submitted for publication, arXiv:1811.01583v1 [cs.IT].
[4] F. Gursoy, I. Siap and B. Yildiz, Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$, *Adv. Math. Commun.* **8**(3), 313-323 (2014).
[5] H. Islam and O. Parkash, Skew cyclic codes and skew $(\alpha_1+u\alpha_2+v\alpha_3+uv\alpha_4)$-constacyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, *Int. J. Information and Coding Theory* **5**(2), 101-116 (2018).
[6] H. Islam, R. K. Verma and O. Parkash, A family of constacyclic codes over $\mathbb{F}_{p^m}[v,w]/\langle v^2-1, w^2-1, vw-wv\rangle$, *Int. J. Information and Coding Theory,* in press.

[7] LI JIN, Skew cyclic codes over ring $\mathbb{F}_p + v\mathbb{F}_p$, *Journal of Electronics (China)* **31**(3), 227-231 (2014).
[8] M. SHI, T. YAO AND P. SOLé,, Skew cyclic codes over a non-chain ring, *Chinese journal of Electronics,* **26**(3), 544-547 (2017).
[9] T.YAO, M.SHI, AND P. SOLé,, Skew cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, *J. Algebra Comb. Discrete Appl.,* **2**(3), 163-168 (2015).

PD-sets for partial permutation decoding of $\mathbb{Z}_{2^s}$-linear Hadamard codes

Mercè Villanueva[1] [merce.villanueva@uab.cat]

[1] Dept. of Information and Communications Engineering,
Universitat Autònoma de Barcelona, Barcelona, Spain

Let $\mathbb{Z}_{2^s}$ be the ring of integers modulo 2^s with $s \geq 1$, and let $\mathbb{Z}_{2^s}^n$ be the set of n-tuples over $\mathbb{Z}_{2^s}$. A nonempty subset $\mathscr{C}$ of $\mathbb{Z}_{2^s}^n$ is a $\mathbb{Z}_{2^s}$-additive code if $\mathscr{C}$ is a subgroup of $\mathbb{Z}_{2^s}^n$. Note that, when $s = 1$, $\mathscr{C}$ is a binary linear code; and when $s = 2$, it is a quaternary linear code or a linear code over $\mathbb{Z}_4$. The $\mathbb{Z}_{2^s}$-additive codes can be seen as binary codes (not necessarily linear) under a generalization of the usual Gray map, $\Phi : \mathbb{Z}_{2^s}^n \to \mathbb{Z}_2^{n2^{s-1}}$ [5,6]. The binary image $C = \Phi(\mathscr{C})$ is a $\mathbb{Z}_{2^s}$-linear code of length $n2^{s-1}$. Permutation decoding is a technique, first introduced for linear codes, that involves finding a special subset, called a PD-set, of the automorphism group of a code. In [3], a new permutation decoding method for $\mathbb{Z}_4$-linear codes and, in general, for systematic codes (not necessarily linear) was introduced, but the determination of PD-sets for nonlinear codes remained an open problem. In [1,2], s-PD-sets of minimum size $s+1$ for some families of nonlinear systematic codes such as $\mathbb{Z}_4$-linear Hadamard, Kerdock and simplex codes are given. We will show the generalization of some of these results to the family of $\mathbb{Z}_{2^s}$-linear Hadamard codes [4,6]. Moreover, we also determine the permutation automorphism group of the corresponding $\mathbb{Z}_{2^s}$-additive Hadamard codes.

Keywords
Permutation decoding, $\mathbb{Z}_{2^s}$-linear codes, Hadamard codes

References

[1] R. D. Barrolleta; M. Villanueva, Partial permutation decoding for binary linear and $\mathbb{Z}_4$-linear Hadamard codes. *Des. Codes Cryptography* **86**(3), 569–586 (2018).
[2] R. D. Barrolleta; M. Villanueva, Partial permutation decoding for several families of linear and $\mathbb{Z}_4$-linear codes. *IEEE Trans. Information Theory* **65**(1), 131–141 (2019).
[3] J. J. Bernal; J. Borges; C. Fernández-Córboda; M. Villanueva, Permutation decoding of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. *Des. Codes and Cryptography* **76**(2), 269–277 (2015).
[4] C. Fernández-Córdoba; C. Vela; M. Villanueva, On $\mathbb{Z}_{2^s}$-linear Hadamard codes: kernel and partial classification. *Des. Codes Cryptogr.* **87**(2-3), 417–435 (2019).
[5] C. Carlet, $\mathbb{Z}_{2^k}$-linear codes. *IEEE Trans. Inform. Theory* **44**(4), 1543–1547 (1998).
[6] D. S. Krotov, On $\mathbb{Z}_{2^k}$-dual binary codes. *IEEE Trans. Inform. Theory* **53**(4), 1532–1537 (2007).

S5 - Computer Algebra for Dynamical Systems and Celestial Mechanics

Influence of Relativistic Effects on the Evolution of Triple Black Hole Systems

Ariel Chitan[1] **, *Shirin Haque***[1] [ariel.chitan@my.uwi.edu]

[1] Physics Department, University of the West Indies, Trinidad, W.I.

The evolution of triple black hole systems was studied using the number of binary interactions occurring during the lifetimes of such systems as one of the parameters. The initial conditions that were varied to change the influence of relativistic effects were the masses of the black holes. Mathematical modelling was implemented with the use of computer simulations on FORTRAN. The code for numerical integration of the equations of motion with post-Newtonian corrections up to 7th order, written by Prof. Seppo Mikkola, was used for the integration of orbits of triple black holes [1],[2]. Black holes, with zero initial velocity, were placed at the vertices of Pythagorean triangles. This was done as a continuation of the study conducted in [3] where the (3,4,5) triangle was analysed as started by the classic Burrau paper [4]. Sixteen Pythagorean configurations were used, all with c<100. For each of the sixteen triangles, masses of the black holes were varied from 10 to 10^{12} Solar masses, forming 12 cases per one triangular configuration. The lifetime of the system and the number of binary encounters in each of the individual cases were found. Orbital plots were also made for comparative purposes. Results indicate that supermassive cases demonstrate shorter lifetimes with orderly behavior and fast mergers while the less massive cases typically are longer lasting and demonstrate more binary interactions and more complicated orbits.

Keywords
Three body problem, Relativistic effects, Black holes

References

[1] S. Mikkola; K. Tanikawa, Implementation of an efficient logarithmic-Hamiltonian three body code. *New Astronomy* **Volume 20**, 38–41 (2013).
[2] S. Mikkola; K. Tanikawa, Regularizing dynamical problems with the symplectic logarithmic Hamiltonian leapfrog. *Monthly Notices of the Royal Astronomical Society* **Volume 430** (Issue 4), 2822–42827 (2013).
[3] M. J. Valtonen, S. Mikkola, H. Pietilä, Burrau's three-body problem in the post-Newtonian approximation. *Monthly Notices of the Royal Astronomical Society* **Volume 273** (Issue 3), 751–754 (1995).
[4] C. Burrau, Numerische Berechnung eines Spezialfalles des Dreikörperproblems. *Astronomische Nachrichten* **Volume 195** (Issue 6), 113–118 (1913).

On the dynamical system generated by the three-body integrator

***Alija Martynova*[1] , *Aleksandr Mylläri*[2] , *Aleksandr Shneivais*[3]** [amyllari@sgu.edu]

[1] St. Petersburg State Forestry University, St. Petersburg, Russia
[2] St. George's University, Grenada, West Indies
[3] St. Petersburg State University, St. Petersburg, Russia

We study the dynamical system generated by the numerical integrator of the three-body problem. Popular three-body code Triple by S. Aarseth is used with untypically small accuracy parameter, of the order of 10^{-16}, while recommended values are of the order of 10^{-12}. Such a small values of accuracy lead to fast accumulation of the round-off errors and strange effects: for some trajectories "quantum leaps" of energy are observed – total energy of the triple system changes tenfold, but after a while returns to original values; sometimes "travel back in time" is observed, etc. These effects are computer- and compiler- dependent and disappear if one makes all constants in use of the proper (double) precision.

Keywords
Three-body problem, Numerical integration of ODE

On the complexity of finite sequences

Aleksandr Mylläri*[1] *, Tatiana Mylläri*[1] *,
***Anna Myullyari*[2] *, Nikolay Vassiliev*[3]** [anna.myullyari@qio.io]

[1] St. George's University, Grenada, West Indies
[2] QiO, Miami, Florida, USA
[3] V.A. Steklov Institute of Mathematics of the Russian Academy of Sciences, St. Petersburg, Russia

We study the complexity of the finite sequences that were constructed numerically by integrating equations of motion of the equal mass free-fall three-body problem. We construct symbolic sequences using close binary approaches, in which the corresponding symbol in the sequence is the number of the distant body. Different approaches to estimate complexity are considered: Shannon entropy, Markov entropy, Kolmogorov complexity and Arnold complexity.

As an estimation of the Kolmogorov complexity we use the length of the archive of the symbolic sequence. Arnold complexity is based on the first differences of the sequences. We compare the results obtained via different methods.

Keywords
Complexity of finite sequences, Three-body problem

Using a CAS-developed random samples generator for teaching and research in probabilistic cellular automata and Statistics

***Gabriel Aguilera-Venegas*[1], *José L. Galán-García*[1], *María Á. Galán-García*[1], *María Galán-Luque*[1], *Yolanda Padilla-Domínguez*[1], *Pedro Rodríguez-Cielos*[1]** [gaguilera@uma.es]

[1] University of Málaga, Málaga, Spain

Our group introduced random samples generation using a CAS, specifically Derive, in the Derive session of ACA 2009. This talk was extended in a paper published in The Derive Newsletter [1]. In the year 2017 we presented a new version focused on research of the random samples generator in STATA that was communicated in [2]. Now a new version of the generator is being implemented in Python with the symbolic pack Simpy. In this case, our we are mainly focused in education.We are now researching in extensions of the Conway's Game of Life, specifically using probabilistic cellular automata. Our long-term goal is the simulation of the growth of cancerous tissues. We have supervised a master thesis with the preliminary works in this topic. For the generation of random numbers involved in the probabilistic automata of this work, we have used the results developed in the previous mentioned work. A summary of this work is about to be published in Advances in Computational Mathematics [3]. This work is both, an education and a research experience for the student who carried out the master thesis. Moreover, the experience of teaching the subject Statistics to engineering students using the material developed for random samples generation has turned out to be useful in the teaching and learning process. The marks obtained in this subject by the students are statistically significantly better than the marks obtained by students of the same subject in others group of engineering where this material has not been used. A brief statistical study about the situation is carried out.

Keywords
Random samples generation, probabilistic automata, Game of Life, CAS.

References

[1] J.L. Galán, G. Aguilera, P. Rodríguez, Y. Padilla, M.A. Galán, *Random distributions.mth: Random samples from distributions with Derive.* The Derive Newsletter, 75, pages: 22-43, 2009. I.S.S.N.: 1990-7079.

[2] G. Aguilera, J.L. Galán, M.A. Galán, P. Rodríguez, R. Rodríguez, *Random samples generation with Stata from continuous and discrete distributions* Proceedings of the 2017 Spanish Stata Users Group meeting. Madrid. October 19, 2017.

[3] G. AGUILERA-VENEGAS; J. L.GALÁN-GARCÍA; R. EGEA-GUERRERO, M. Á. GALÁN-GARCÍA, P. RODRÍGUEZ-CIELOS, Y. PADILLA-DOMÍNGUEZ, M. GALÁN-LUQUE, A probabilistic extension to Conway's Game of Life *Advances in Computational Mathematics* (in press).
DOI: `https://doi.org/10.1007/S10444-019-09696-8`.

Dynamic Applications for Learning and Exploring Mathematics Using Computer Algebra

William Bauldry[1] **,** ***Wade Ellis***[2] [BauldryWC@appstate.edu]

[1] Mathematical Sciences, Appalachian State University, Boone, NC.
[2] Mathematics Department, West Valley College, Saratoga, California.

We discuss designing self-contained electronic documents that form a microworld for student investigations; we call these ACR documents. The documents include a CAS application in which students engage in 'sandboxed' mathematical exploration. The inquiry-based exploration is led by a set of questions in the document that guide students, experimenting in the computer algebra and dynamic geometry microworlds, that are formulated under the *Action-Consequence-Reflection paradigm.*

The *Action-Consequence-Reflection paradigm* is a research-based pedagogical approach that provides students with a microworld in which to take a mathematical action, observe the consequences of their action, and reflect on the observed behaviour in order to construct mathematical understanding. This paradigm is the basis of the $\Delta\mu$ project which constructed several exemplars and templates for faculty.

We will begin our session with examples of ACR documents, the student exercises/projects that they support, and instructor guides. A screenshot of a sample ACR document is shown in Figure 1. Then we will move to discussing how to construct ACR documents using Maple 2019

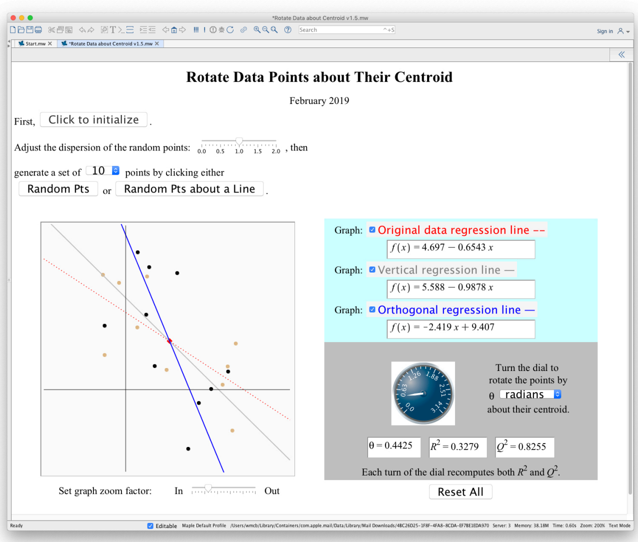


Figure 1: Linear Regression ACR Maple 2019 Worksheet

or TI Nspire as our computer algebra substrates. Last, we discuss formulating questions that are the crucial part of the project for students. We'll close with pointers to further information and participant discussion & questions.

Keywords
Dynamic computer algebra pedagogical applications, Action-Consequence-Reflection paradigm

References

[1] D. APPLE and W. ELLIS, "Learning how to learn: Improving the performance of learning," Int'l J of Process Education, 7(1), 2015, 21-28.
[2] G. BURRILL, "The Role of Handheld Technology in Teaching and Learning Secondary School Mathematics," ICME 11, TSG-22. Monterrey, México, 2008.
[3] T. DICK, G. BURRILL, and G. BRADY, "New technologies offer new ways to engage students," NCSM Newsletter, 38 (2007).
[4] W. ELLIS, "Technology and Calculus." In *Calculus Renewal: Issues for Undergraduate Mathematics Education in the Next Decade*, 53-68, S. Ganter (ed), Springer US, Boston, 2000.
[5] W. ELLIS, W. BAULDRY, M. BOSSÉ, and S, OTEH, "Employing Technology to Visualize Complex Roots of Real Polynomials," Electronic Proc. of TIME-2016, UNAM, México City, Jan. 2017.
[6] W. BAULDRY, "Using Maple in Modern Algebra and Advanced Calculus Courses," Proc. of the 20th Annual ICTCM, 2009, 13-17.
[7] E. MARLAND, G. RHOADS, M. BOSSÉ, J. SANQUI, and W. BAULDRY, "Q^2: A Measure of Linearity," (submitted, Feb., 2019).

Exciting Updates to the TI-Nspire™ World
(Part I, Part II)

Gosia Brothers[1] [gbrothers@ti.com]

[1] Product Manager, MGTS, Texas Instruments, Dallas, TX, USA

The Texas Instruments development team has been working hard to improve our TI-Nspire™ platform. Based on your requests and feedback, we have implemented new and exciting updates to the TI-Nspire™ CX graphing calculators and software. Please come to this session to learn what's new.

Assessment Tools in Maple: Recent Developments and Challenges

Paulina Chin[1]**, *Paul DeMarco***[1] `[pchin@maplesoft.com]`

[1] Maplesoft, Waterloo, Ontario, Canada

The benefits of using computer algebra systems to demonstrate and explore mathematical concepts are clear. However, the use of a CAS for assessment in mathematics and science courses still poses a number of challenges. In this presentation, we will show several recent additions to the Maple [1] software package for the purposes of grading and self-assessment, and our focus will be on the design issues we encountered in building the tools as well as the challenges we face in their future development.

One of these tools is the graph assessment tool in Maple's Grading package. Its purpose is to allow "sketches" of plots entered by students into a computer to be compared to ones requested by an instructor. Issues that we needed to consider in our design that continue to pose difficulties include noise in the data points, scaling of test questions, and questions that do not have unique solutions.

We will also present and discuss the Quiz command in the Grading package, which is intended to generate randomized quizzes on a variety of mathematical subjects, with automated assessment of the answers. The challenges in the design of this tool include going beyond simple multiple-choice questions and providing an easy-to-use interface that allows instructors to focus on the mathematical concepts rather than programming-like syntax for authoring the questions.

Finally, we will show the EssayTools package, which contains tools related to the assessment of essays. Though they are not meant for the assessment of mathematics, the algorithms were easily implemented using the functionality a CAS offers.

Keywords
software, assessment, education, Maple

References

[1] Maple 2019, `www.maplesoft.com/products/maple`

DGS assisted activities around the Golden Ratio in Space and Time

***Thierry Dana-Picard*[1], *Sara Hershkovitz*[2]** [ndp@jct.ac.il]

[1] Department of Mathematics, Jerusalem College of Technology, Jerusalem, Israel
[2] Center for Educational Technology, Tel Aviv, Israel

Mario Livio [4] wrote that "The history of art shows that in the long search for an elusive canon or “perfect” proportion, one that would somehow automatically confer aesthetically pleasing qualities on all works of art, the Golden Ratio has proven to be the most enduring". This Golden Ratio is defined as follows.

Consider a segment AB and a point C on this segment, as in Figure 1.

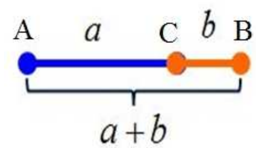


Figure 1: Harmonious divide of a segment

Denote $a = AC$ and $b = CB$. Then the division of the segment is made according to the Golden Ratio if

$$\frac{a+b}{a} = \frac{a}{b}.$$

It is easily shown that this ratio is equal to $\frac{1+\sqrt{5}}{2}$, and is denoted by the Greek letter ϕ. Traditionally, the ancien Greeks are credited for this choice. Koshy [5] writes that the letter ϕ has been chosen in honor of the sculptor Phidias by the American Mathematician Mark Barr. In Chapters 20-21, Koshy mentions other reasons for the choice of this Greek letter. He refers to Coxeter for an explanation why this number has been also denoted by the Greek letter τ, the first letter of the Greek word $\tau o \mu \eta$ (section).

Actually, there are occurrences of the Golden Ratio in more ancient sources. It appears in the Bible, and recently, ancient jewelry and objects related to observation of planets have been discovered in chalcolithic archeological sites near Varna, Bulgaria. Activities around the Golden Section may be developed for every age of students. For each category of students, technology may be used. Among them:

1. The geometry of plane configurations, leading to the study of specific buildings. We will show the Golden Ration appearing in an Italian octagonal Middle Ages castle and in a 19^{th} century synagogue in Budapest, Hungary. The experiments have been made

using GeoGebra[†], a free downloadable Dynamical Geometry System (DGS). This is a good opportunity to apply a specific feature of GeoGebra for augmented reality.

2. The Golden Ratio appears also when studying the graphs of trigonometric functions and their tangents; see Figure 2. This can be studied using a CAS.

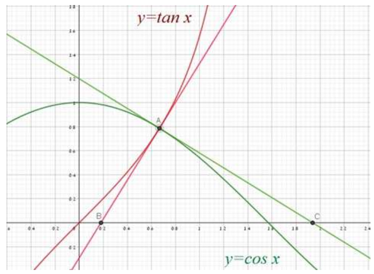


Figure 2: Tangents to the graphs of trigonometric functions

3. The determination of the center of mass of earrings made when cutting off a disk form another disk, in a certain configuration. In this case, double integrals have to be computed. A Computer Algebra System has been used.

4. In music, a non-geometric setting, specific accords are determined by frequency ratios equal to specific ratio of Fibonacci numbers. This can be checked using a CAS. Of course of full experiment would requires other kinds of technology, available in an acoustic lab.

5. Geometry and acoustics may be connected with a study of the shapes of various instruments. This study may be performed using a DGS.

6. The needed computations for the traditional Hebrew calendar, which is lunar-solar[‡] are based on the so-called Meton formula. This formula reads: $12 \cdot 12 + 7 \cdot 13 = 235$. Actually, the number of days in 235 lunations is equal to the number of days in 19 tropical years. In order for the High Holidays to be in phase with the seasons, the Hebrew calendar is organized in cycles of 19 years, where 12 years are regular (12 months each) and 7 of them are 13-month years. This also leads to the appearance of the Golden Ratio in a non-geometric setting. It must be noted that, as the interval between two consecutive new moons is not an integer, neither is the number of days in a tropical year, Meton formula is not enough for establishing a calendar. Historically, these computations have been made by hand, but technology makes them easier.

For some of these examples, we will present technology based activities which have been proposed to students of various ages, some of them undergraduates, but the last one with K5 students.

[†]`https://www.geogebra.org/`

[‡]Unlike the Gregorian calendar, which is purely solar, and unlike the Muslim calendar, which is purely lunar.

Keywords
Golden Ratio, DGS, CAS

References

[1] TH. DANA-PICARD; S. HERSHKOVITZ, A Glimpse at Mathematics in Jewish Traditional Artefacts, *Symmetry: Culture and Science*, **29**(2), 307-317 (2018).
[2] TH. DANA-PICARD; S. HERSHKOVITZ, Geometrical Features of a Jewish Monument: Study with a DGS. To appear in *the Journal of the Mathematics and the Arts* (2019).
[3] TH. DANA-PICARD, *Rabbits, beauty and kindness – on mathematics and aesthetics: the hidden hand in nature*, in *(*TDP and G. Morali, edts) Ladaat Baarets Darekkha Vol. I , JCT and Bet-El Library Publishers, 69-96 (2017). In Hebrew.
[4] M. LIVIO, , *The Golden Ratio: The Story of Phi, the World's Most Astonishing Number*. Broadway Books, New York, 2002.
[5] TH. KOSHY. *Fibonacci and Lucas Numbers with Applications*, J. Wiley, New York, 2001.

Parametric integrals, combinatorial identities and applications

***Thierry Dana-Picard*[1] , *David G. Zeitoun*[2]** [ndp@jct.ac.il]

[1] Department of Mathematics, Jerusalem College of Technology, Jerusalem, Israel
[2] Orot Israel College, Elkana, Israel

We propose a survey of parametric integrals (aka sequences of definite integrals) studied by undergraduates in an engineering school and pre-service teachers, in a technology-rich environment. The papers in reference provide a few examples only. Parametric integrals are interesting both for their mathematical properties, and the numerous applicable methods, and for their importance in applied science; see [1].

Let be given an either definite or improper integral of the so-called second type

$$I_n = \int_a^b f_n(t)\, dt,$$

where $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$ are given. The study of the family of integrals I_n can yield the following results:

1. An induction formula for the sequence (I_n), such as $I_{n+1} = R(n) I_n$ or $I_{n+1} = u_n + R(n) I_n$, etc., where $R(n)$ is a function of the parameter n; see [2,3,4,5,6].
2. A closed formula for I_n as a function of the parameter n, often using telescoping methods which lead to factorial expressions. This is the case if $R(n)$ is a rational function. In some cases, induction connects I_{n+2} and I_n, and the usage of double factorials may yield more compact formulas. Otherwise, the study of the convergence of a series is necessary.
3. Combinatorial identities, in the case where more than one integration method can be applied.
4. New integral presentations of classical combinatorial numbers; see [3,4,5]

Technology contributes to the study in various ways.

1. A Computer Algebra System provides often an interactive tutor for integration methods. Its usage for small values of the parameter helps to find a general way to compute I_n as a function of $I_{n-1}, I_{n-2}, \ldots$. With this, closed formulas can be looked for.
2. The Online Encyclopedia of Integer Sequences (`oeis.org`). Experiments with the CAS provide the first terms of the sequences of integrals. Using the database, candidates to describe the sequence (I_n) are obtained. Determination of a closed formula is made easier.

Specific situations may appear:

- The computation of the integral for general parameter may be performed directly by the CAS. This has been the case for $I_n = \int_0^{\pi/2} \frac{dt}{1+tan^n(t)}$ with DERIVE (it returns immediately $\pi/4$, an answer independent of the value of the parameter!). Other CAS had hard time with this integral. The reason is that a specific theorem is implemented there; this theorem does not appear in most textbooks and is explained in [1].
- If the answer is readable immediately, we are done. The answer may involve special functions. For example, if $I_n = \int_0^{\pi/2} \sin^n t \, dt$, Maple's command returns immediately $I_n = \frac{\sqrt{\pi}\,\Gamma(\frac{1}{2}+\frac{n}{2})}{2\,\Gamma(1+\frac{n}{2})}$, providing an incitement to learn something new, the Gamma function, as an extension of the curriculum. An example is described in [5].

We illustrate the different cases with new examples of integrals of rational functions, trigonometric functions, etc., and examples of applications in science and engineering.

Keywords
Parametric integrals, combinatorics, applications

References

[1] G. Boros and V. Moll, *Irresistible Integrals: Symbolics, Analysis And Experiments In The Evaluation Of Integrals*, Cambridge University Press (2004).
[2] Th. Dana-Picard, Parametric integrals and symmetries of functions, *Mathematics and Computer Education*, 5-12 (2005).
[3] Th. Dana-Picard, Integral presentations of Catalan numbers and Wallis formula, *International Journal of Mathematical Education in Science and Technology* **42** (1), 122-128 (2011).
[4] Th. Dana-Picard and D.G. Zeitoun, Sequences of definite integrals, infinite series and Stirling numbers, *International Journal of Mathematical Education in Science and Technology* **43** (2), 219-230 (2012).
[5] Th. Dana-Picard and D.G. Zeitoun, Parametric integrals, Wallis formula and Catalan numbers, *International Journal of Mathematical Education in Science and Technology* **43** (4), 515-520 (2012).
[6] Th. Dana-Picard and D.G. Zeitoun, Exploration of Parametric Integrals related to a Question of Soil Mechanics, *International Journal of Mathematical Education in Science and Technology* **48** (4), 617-630 (2017).
[7] P. Glaister, Factorial sums, *International Journal of Mathematical Education in Science and Technology* **34** (2), 250-257 (2003).

SFOPDES: A stepwise tutorial for teaching Partial Differential Equations using a CAS

***Gabriel Aguilera-Venegas*[1] , *José Luis Galán-García*[1] ,**
***María Ángeles Galán-García*[1] , *Yolanda Padilla-Domínguez*[1] ,**
***Pedro Rodríguez-Cielos*[1] , *Ricardo Rodríguez-Cielos*[2]** `[jlgalan@uma.es]`

[1] University of Málaga, Málaga, Spain
[2] Technical University of Madrid, Madrid, Spain

Partial Differential Equations (PDE) are one of the most difficult topics that Engineering and Sciences students have to study in the different Math subjects in their degree.

In this talk we introduce `SFOPDES` (Stepwise First Order Partial Differential Equations Solver) aimed to be used as a tutorial for helping both the teacher and the students in the teaching and learning process of PDE.

The type of problems that `SFOPDES` solves can be grouped in the following three blocks:

1. **Pfaff Differential Equations**, which consists on finding the general solution for:

$$P(x,y,z)\,\mathrm{d}x + Q(x,y,z)\,\mathrm{d}y + R(x,y,z)\,\mathrm{d}z = 0$$

   a) General method.

   b) Particular cases:

      i. Separable equations.

      ii. Exact Pfaff equations.

      iii. One-separated variable equations.

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

   a) General method.

   b) Particular solution which contents a given curve Γ.

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

   a) General method.

   b) Particular cases:

      i. $F(p,q) = 0$

ii. $g_1(x,p) = g_2(y,q)$

iii. $z = px + qy + g(p,q)$

In [1], a talk given at ACA 2018 conference, we introduced the first version of this tutorial where the general methods for each type of the above PDE were considered. In this talk we extend that work introducing new programs which solve the particular cases of Pfaff equations and general first order PDE using Lagrange-Charpit method.

We have used the CAS DERIVE to develop this tutorial since Engineering students at the University of Málaga are still using this software in the computer lectures in different topics. The way of using this CAS in teaching has been shown in previous ACA conferences and in published papers as [2] or [3].

Nevertheless, since DERIVE is discontinued, we are migrating this tutorial to a free and multi-platform environment as PYTHON programming language using SYMPY which is a CAS extension for PYTHON. This way, the tutorial will be available for any user without the need of a proprietary software as DERIVE. In this talk, we will also show the advances (with the advantages and disadvantages) in this migration. In addition, this migration to PYTHON will allow it uses in the SAGEMATH since this free CAS can deals with the PYTHON library SYMPY.

Keywords
PDE, Stepwise tutorial, CAS, DERIVE, SYMPY, PYTHON, SAGEMATH

References

[1] J.L. GALÁN-GARCÍA, P. RODRÍGUEZ-CIELOS, Y. PADILLA-DOMÍNGUEZ, M.Á. GALÁN-GARCÍA, G. AGUILERA-VENEGAS, R. RODRÍGUEZ-CIELOS, Teaching Partial Differential Equations with CAS. In *24th Conference on Applications of Computer Algebra - ACA 2018*, Francisco Botana, Felipe Gago and Manuel Ladra (eds.), 64–65. Servizo de Publicacións e Intercambio Científico Campus Vida, Santiago de Compostela (Spain), 2018, ISBN 978-84-16954-87-2.

[2] G. AGUILERA-VENEGAS, J. L. GALÁN-GARCÍA, M. Á. GALÁN-GARCÍA, P. RODRÍGUEZ-CIELOS, Teaching semantic tableaux method for propositional classical logic with a CAS. *International Journal for Technology in Mathematics Education* **22**(2), 85–92 (2015).

[3] G. AGUILERA-VENEGAS, J. L. GALÁN-GARCÍA, M.Á. GALÁN-GARCÍA, G. LOBILLO-MORA, J. MARTÍNEZ-DEL-CASTILLO, S. MERINO-CÓRDOBA, Y. PADILLA-DOMÍNGUEZ, P. RODRÍGUEZ-CIELOS, R. RODRÍGUEZ-CIELOS, Parametrization of curves and line integrals with a CAS. *International Journal for Technology in Mathematics Education* **24**(4), 179–190 (2017).

Teaching the residue theorem and its applications with a CAS

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

[1] Applied Mathematics, University of Málaga, Málaga, Spain

The residue theorem is one of the most interesting result in Complex Analysis which allows not only computations in $\mathbb{C}$, the Field of Complex Numbers, but also provides many applications in the Field of Real Numbers $\mathbb{R}$.

In [1] we introduced the file `RESIDUE.MTH`, developed in the CAS DERIVE which main objective was to provide tools for solving integration problems in Complex Analysis using the residue theorem.

In this talk we present the library `ResidueApplications`, that was initially developed in DERIVE since Engineering students in the University of Málaga are still using this software in computer lectures. However, we are migrating this library to PYTHON using the symbolic mathematics library SYMPY. This way it will be also possible to use this package in other CAS as SAGEMATH.

The main goals of the `ResidueApplications` library are not only to provide some important applications of the Residue theorem but also to use it as a pedagogical tool for Engineering students.

`ResidueApplications` can be used as a tutorial in the teaching and learning process of this topic since it provides the results step by step allowing the students to check their computations when they solve an exercise. When developing this package, we were not interesting only in the computations of residues and their applications (which can be easily done using standards functions in different CAS) but mainly on its pedagogical use. In addition of the step by step facility, using this library, the students also can develop their own programs to deal with different applications. This way, the student are the protagonist of their self-learning process. For example, If the students develop a program to compute the residues of a function, they will be better prepared to understand this topic.

The programs developed in this tutorial can be grouped in the following blocks:

1. Compute of residues.
2. Compute of complex integrals using the residue theorem.
3. Applications of the residue theorem to compute integrals in $\mathbb{R}$:
    a) Trigonometric integrals.
    b) Improper integrals.

In previous ACA conferences we dealt with the application of the residue theorem to compute improper integrals (see [1] and [2]). In this talk, although we will present an overview of the whole tutorial, we will focus mainly in the computation of trigonometric integrals.

Keywords
Residue theorem, Trigonometric integrals, Improper integrals, Stepwise tutorial, CAS, DERIVE, PYTHON, SYMPY

References

[1] J.L. GALÁN-GARCÍA, M.Á. GALÁN-GARCÍA, Y. PADILLA-DOMÍNGUEZ, P. RODRÍGUEZ-CIELOS, 91. Residue.mth: solving problems of integration using the residue theorem. In *Proceedings of TIME-2004 Symposium: Technology and its Integration in Mathematics Education*, Montreal (Canada), 2004, ISBN 3-901769-59-5.
[2] G. AGUILERA, J.L. GALÁN, M.A. GALÁN, Y. PADILLA, P. RODRÍGUEZ, R. RODRÍGUEZ, 15. Teaching improper integrals with CAS. In *21st Conference on Applications of Computer Algebra - ACA 2015*, 90–91. Kalamata (Greece), 2015, ISBN 978-84-16954-87-2.
[3] J.L. GALÁN-GARCÍA, G. AGUILERA-VENEGAS, P. RODRÍGUEZ-CIELOS, Y. PADILLA-DOMÍNGUEZ, M.Á. GALÁN-GARCÍA, 2. New rules for improving CAS capabilities when computing improper integrals. Applications in Math Education. In *24th Conference on Applications of Computer Algebra - ACA 2018*, Francisco Botana, Felipe Gago and Manuel Ladra (eds.), 63–63. Servizo de Publicacións e Intercambio Científico Campus Vida, Santiago de Compostela (Spain), 2018, ISBN 978-84-16954-87-2.

Realizing the concept of "Multiple Representations" by using CAS (Part I, Part II)

Helmut Heugl[1] [hheugl@aon.at]

[1] Head of ACDCA (Austrian Center for Didactics of Computer Algebra)

Mathematical concepts are presented in multiple modes of representation (or "prototypes") such as text, graphs and diagrams, tables, algebraic expressions and computer simulations. A prime goal of teaching is to help learners develop an understanding of the mathematical concepts by considering and using these different representational modes and levels. Several prototypes of the concept provide complementary information [1]. Therefore it is not enough to become acquainted with and to understand the information of a certain representation mode. A central cognitive activity on the way to mathematical concepts is to build links between representation modes of a concept. In traditional mathematics education prototypes mostly are available in a serial way. The main importance of technology tools is that the learner can use several prototypes parallelly. By using examples of Algebra and Analysis I will show the role of CAS when building links between several representation modes of a concept or when solving problems [2].

References

[1] DÖRFLER, W., Der Computer als kognitives Werkzeug und kognitives Medium. In *Computer - Mensch – Mathematik. Verlag Hölder-Pichler-Tempsky*, Wien, 1991, pp51. ISBN3-209-01452.

[2] HEUGL, H., Mathematikunterricht mit Technologie – ein didaktisches Handbuch mit einer Vielzahl von Aufgaben. *Veritas-Verlag*, Linz, 2014, ISBN 978-3-7101-0431.

Interactive tutorials, an example on symmetric functions

***Pauline Hubert*[1], *Mélodie Lapointe*[1]** [hubert.pauline@courrier.uqam.ca]

[1]Département de Mathématiques, Université du Québec à Montréal, Montréal, Canada

Sage is a free open source computer algebra software. The project was started in 2005 by William Stein [2] as an open source alternative to mathematical systems such as Maple or Mathematica, and is based on python and many existing open-source packages. Thanks to its hundreds of worldwide contributors, Sage now contains a large variety of libraries such as calculus, linear algebra, combinatorics, number theory, and it is used intensively in research and higher education.

Current tutorials and documentation are often written by top specialists in their fields, because of this, it can be hard to access for newcomers. Thus, we wanted to build a tutorial which is both a mathematical introduction to the subject, and a tutorial on how to use the relevant tools in Sage.

In our case, we have been mostly interested in the symmetric function tools. The classical mathematical reference here is [1]. Our goals were to improve and complete the pre-existent tutorials, to add an interactive dimension and to show the mathematics behind and not only the Sage tools. The expected result would thus interlace class notes with an actual tutorial on how to use Sage to explore the notions considered.

In this presentation, we will use the example of this tutorial to present some interesting features of Sage and Jupyter. We will also talk about how interactive tutorials and notebooks may be turned into learning tools. One of the key features here is the closeness between the mathematical development of the subject considered and the Sage programming style.

Keywords
Interactive tutorial, Sage, Symmetric functions

References

[1] I. G. MACDONALD, *Symmetric functions and Hall polynomials.* Oxford University Press, New York, 1995.
[2] W. STEIN, Sage: creating a viable free open source alternative to Magma, Maple, Mathematica, and MATLAB. *London Math. Soc. Lecture Note Ser.* **403**, 230–238 (2013).

Innovative CAS Technology Use in University Mathematics Teaching and Assessment: Findings from a Case Study in Alberta, Canada

***Chantal Buteau*[1], *Charles Doran*[2],**
***Daniel Jarvis*[3], *Andrey Novoseltsev*[2]** [danj@nipissingu.ca]

[1] Faculty of Mathematics and Science, Brock University, St. Catharines, Ontario, Canada
[2] Faculty of Mathematical and Statistical Sciences, University of Alberta, Edmonton, Alberta, Canada
[3] Schulich School of Education, Nipissing University, North Bay, Ontario, Canada

In this presentation, I will discuss a recent journal publication [1] in which we report on a case study that focused on innovative uses of CAS technology in university mathematics teaching and assessment. The research study involved a site visit to the University of Alberta campus during which: interviews we re conducted with five mathematics faculty members and seien mathematics students; math lectures were attended; and artifacts were collected such as course outlines, software demonstrations, and assessment tools. Interviews were transcribed and the data entered into Atlas.ti qualitative research software for the purpose of thematic analysis. Findings center around the innovative use of the open source software known as SageMath, both in the teaching (answer checking, interactive lecture demonstrations) and assessment (assignments, mid-terms, final examinations) practices of one particular instructor who taught seven iterations of a Mathematical Programming and Optimization undergraduate course.

Keywords
mathematics education, technology, Computer Algebra Systems (CAS), teaching, assessment

References
[1] D. H. Jarvis, C. Buteau, C. Doran and A. Novoseltsev, Innovative CAS technology use in university mathematics teaching and assessment: Findings from a case study in Alberta, Canada. *Journal of Computers in Mathematics and Science Teaching,* **37**(4), 309-354 (2018).

The importance of being continuously continuous

David Jeffrey[1], ***David Stoutemyer***[2] [djeffrey@uwo.ca; dstout@hawaii.edu]

[1] ORCCA, University of Western Ontario, London, Ontario, Canada
[2] Computer Science, University of Hawaii, Hawaii, USA

We discuss two forms of continuity in the context of integration.

The fundamental theorem of calculus requires that the expression for the integral must be continuous on the interval of interest. Computer Algebra systems, however, do not always co-operate with this requirement. Given an integrand that is continuous on an interval, a computer algebra system may not return an expression that is also continuous on the interval. We show how this can happen, how it can be repaired [1], and speculate on why it has not been.

The other type of continuity refers to continuity with respect to parameters. Consider calculus's most famous integral:

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

When $n = -1$, this expression breaks down, but a valid integral still exists, namely $\log(x)$. This can be regarded as a discontinuity in the parameter n. There are many similar integrals whose standard expressions contain parametric discontinuities. We show how such integrals can be made parametrically continuous [2], and demonstrate a program that does this.

Keywords
Integration, Continuity, Kahanian

References

[1] D.J. JEFFREY, The importance of being continuous. *Mathematics magazine*, **67**, 294 - 300, 1994.
[2] W. KAHAN, Personal communication.

Symbolic calculation behind floating-point arithmetic using CAS

Jan Krupa [1] **,** ***Włodzimierz Wojas*** [1] [jan_krupa@sggw.pl]

[1] Department of Applied Mathematics, Warsaw University of Life Sciences (SGGW), Warsaw, Poland

In this talk we would like to present using CAS, some examples of symbolic calculations which lie behind calculations in floating-point arithmetic (with double precision). Each operation in floating-point arithmetic is performed according to a precise-symbolic algorithm. In spite of the fact that floating point arithmetic is based on symbolic operations, it gives approximate results with some exceptions, e.g.: adding, subtracting and multiplying integers; adding, subtracting, multiplying and dividing negative integer powers of 2. We will present in this talk simple examples in Mathematica and wxMaxima where the result of operations may depend on the interpretation of the user input data (numbers) by CAS functions (such as Solve, Limit, Det, solve, limit, det) – as symbolic or approximate. The result may also depend whether these CAS functions use more or less clever algorithms.

Keywords
Higher education, Floating Point Arithmetic, Application of CAS, Mathematica, Mathematical didactics

References

[1] TIMOTHY SAUER, *Numerical Analysis*. 3rd Edition, Pearson, 2017
[2] The GNU MPFR (multiple-precision floating-point computations) Library: `https://www.mpfr.org`
[3] IEEE 754 Floating Point Standard: `https://en.wikipedia.org/wiki/IEEE_754`
[4] D. GOLDBERG, “What Every Computer Scientist Should Know about Floating Point Arithmetic.” ACM Computing Surveys 23, 5–48, 1991
[5] W. STALLINGS, *Computer Organization and Architecture*, 6th ed. Prentice Hall, Upper Saddle River, NJ, 2003.

Some examples of calculation improper integrals using CAS

Jan Krupa[1] **,** ***Włodzimierz Wojas***[1] `[jan_krupa@sggw.pl]`

[1] Department of Applied Mathematics, Warsaw University of Life Sciences (SGGW), Warsaw, Poland

Improper integrals are taught students in framework of such academic courses as: Calculus, Mathematical Analysis or Higher Mathematics as a standard. In this talk we would like to present some didactics examples representing different approaches to calculate improper integrals using Mathematica and wxMaxima. We will present two examples of improper integral calculated using Riemann sums. We will compare Riemann and Lebesgue approaches to integral $\int_0^{\infty} \frac{\sin x}{x}\,\mathrm{d}x$. We will also analyse complex approach to calculate improper integrals on the following examples: $\int_{-\infty}^{\infty} \frac{x^2}{x^6+6x^4+9x^2+4}\,\mathrm{d}x$ and $\int_L \frac{\mathrm{Re}\,z}{\bar{z}}\,\mathrm{d}z$ where L is a broken line ABC on Gauss plane and $A=-1$, $B=0$, $C=i$.

Keywords
Higher education, Improper integrals, Application of CAS, Mathematica, Mathematical didactics

References

[1] I.M. ROUSSOS, *Improper Riemann Integrals*, CRC Press, 2014
[2] JIAN-KE LU, SHOU-GUO ZHONG AND SHI-QIANG LIU, *Introduction to the Theory of Complex Functions*, Series of Pure Mathematics, World Scientific, 2002

Familiarizing students with definition of Lebesgue integral using Mathematica - some examples of calculation directly from its definition: Part 2

Jarosław Bojarski, Jan Krupa[1], Włodzimierz Wojas[1] [jan_krupa@sggw.pl]

[1] Department of Applied Mathematics, Warsaw University of Life Sciences (SGGW), Warsaw, Poland

In popular books of calculus, for example [2, 3], we can find many examples of Riemann integral calculated directly from its definition. The aim of these examples is to familiarize students with the definition of Riemann integral. In this article, with similar aim but for Lebesgue integral definition, we present the following examples of calculation directly from its definition: $\int_0^1 x\chi_{\mathbb{Q}}(x)\,\mathrm{d}m(x)$, $\int_0^\infty e^{-x}\,\mathrm{d}m(x)$, $\int_0^1(-\ln x)\,\mathrm{d}m(x)$, $\int_1^\infty \frac{1}{x}\,\mathrm{d}m(x)$, $\int_0^1 \frac{1}{x}\,\mathrm{d}m(x)$ and some others, $\mathrm{d}m(x)$ denotes the Lebesgue measure on the real line. The title of this talk is very similar to the title of author's article [1] in which there are examples of Lebesgue integrals of bounded function over bounded intervals calculated directly from its definition but in our talk we show examples of Lebesgue integrals of bounded or unbounded function over bounded or unbounded intervals calculated directly from its definition. We calculate sums, limits and plot graphs of needed simple functions using Mathematica. Using Mathematica or others CAS programs for calculation Lebesgue integral directly from its definitions, seems to be didactically useful for students because of the possibility of symbolic calculation of sums, limits - checking our hand calculations and plotting dynamic graphs. Moreover we get students used not only to the definition of Lebesgue integral but also to CAS applications generally.

The two following definitions of Lebesgue integral are used in this article:

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

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

Definition 1. (See [4, 6, 7, 8, 9])

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

Definition 2. (See [5, 10, 11]) Let s_n be nondecreasing sequence of nonnegative simple measurable functions such that $\lim\limits_{n\to\infty} s_n(x) = f(x)$ for every $x \in \mathbb{R}$. Then:

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

Keywords
Higher education, Lebesgue integral, Application of CAS, Mathematica, Mathematical didactics

References

[1] Włodzimierz Wojas and Jan Krupa, Familiarizing Students with Definition of Lebesgue Integral: Examples of Calculation Directly from Its Definition Using Mathematica, *Mathematics in Computer Science*, **11**, 363–381, http://doi.org/10.1007/s11786-017-0321-5, (2017).
[2] Tom M. Apostol, *Calculus, Volume 1, One-Variable Calculus with an Introduction to Linear Algebra*, 2nd ed., Addison-Wesley Publishing Company, (1991).
[3] G. M. Fichtenholz, *Differential and Integral Calculus*, Fizmatgiz, (1958).
[4] W. Rudin, *Principles of Mathematical Analysis*, 3rd ed., McGraw-Hill Education, (1973).
[5] Charalambos D. Aliprantis, Owen Burkinshaw, *Principles of Real Analysis*, 3rd ed., Academic Press, (1998).
[6] Robert G. Bartle, *The Elements of Integration and Lebesgue Measure*, Wiley-Interscience, (1995).
[7] Frank Jones, *Lebesgue Integration On Euclidean Space*, Jones & Bartlett Learning, (2000).
[8] Andrew Browder, *Mathematical Analysis An Introduction*, 2nd ed., Springer, (2001).
[9] Gerald B. Folland, *Real Analysis Modern Technique*, 2nd ed., Wiley, (2007).
[10] W. Kołodziej, *Mathematical Analysis*, (in polish), Polish Scientific Publishers PWN, Warsaw (2012).
[11] R. Sikorski, *Differential and Integral Calculus. Functions of several variables*, (in polish), Polish Scientific Publishers PWN, Warsaw (1977).
[12] H. Ruskeepa, *Mathematica Navigator: Graphics and Methods of applied Mathematics.* Academic Press, Boston (2005).
[13] S. Wolfram, *The Mathematica Book.* Wolfram Media Cambridge University Press (1996).

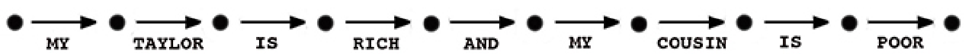
Putting words on arrows and loops

Gilbert Labelle[1] ***, Louise Laforest***[2] `[labelle.gilbert@uqam.ca]`

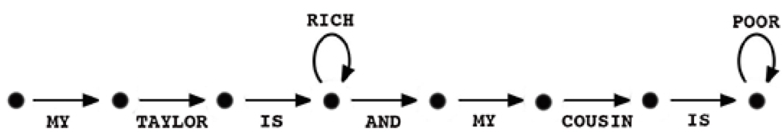
[1] Dép. de mathématiques, U. du Québec à Montréal, Montréal (Québec) Canada
[2] Dép. d'informatique, U. du Québec à Montréal, Montréal (Québec) Canada

THE CONTEXT. We introduced in [1] the general notion of *graphical sentence* as the mathematical object obtained by putting a non empty word (from a finite alphabet $\mathbb{A}$) on each arrow or loop of a connected directed graph. Each word is written according to the direction of its corresponding arrow or loop. The graphs are made of elastic arrows and loops and are not embedded in a plane. We propose a classroom activity for discrete mathematics students having access to a CA system, in which four simple kinds of graphical sentences are to be analyzed, namely the *one-way or two-way linear graphical sentences with or without loops*. Here are samples of graphical sentences belonging to each of these four kinds.

(1a) The kind $\underset{\rightarrow}{\mathscr{L}}$ of one-way linear sentences without loops (i.e., ordinary sentences), e.g.,

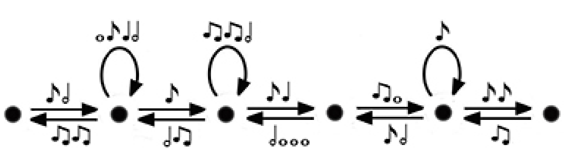


(1b) The kind $\underset{\rightarrow}{\mathscr{L}}^{\circlearrowright}$ of one-way linear sentences with (possible) loops, e.g.,



(2a) The kind $\underset{\rightleftarrows}{\mathscr{L}}$ of two-way linear sentences without loops, e.g.,

(2b) The kind $\underset{\rightleftarrows}{\mathscr{L}}^{\circlearrowright}$ of two-way linear sentences with (possible) loops, e.g.,



the alphabets being the standard (cap) 26-letter alphabet, { ♡, ◇, ♣, ♠ }, { ♪, 𝅗𝅥, ♫, 𝅝, ♩ }.

The finite alphabet $\mathbb{A}$ can be an arbitrary set of symbols and the words put on arrows or loops are mathematical words, i.e., arbitrary finite sequences of "letters" in $\mathbb{A}$. Graphical sentences can be used to encode sets of sentences in a compact way: the *readable sentences* being the sequences of words corresponding to directed paths in the graph, the letters of each word being read from source to target of its corresponding arrow or loop.

For example, the following are readable sentences

Kind $\underset{\rightarrow}{\mathscr{L}}$: "`MY COUSIN IS POOR`".

Kind $\underset{\rightarrow}{\mathscr{L}}^{\circlearrowright}$: "`MY TAYLOR IS RICH RICH RICH AND MY COUSIN IS POOR POOR`".

Kind $\underset{\rightleftarrows}{\mathscr{L}}$: "♣♡ ♠♢ ♣♡ ♠♠ ♢♢♢ ♠♠♠ ♣♢♡".

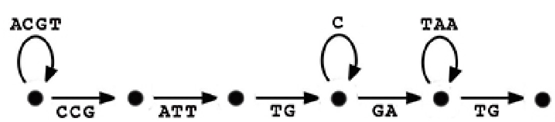
Kind $\underset{\rightleftarrows}{\mathscr{L}}^{\circlearrowright}$: "𝅝♪♩♩ ♪ ♫♩ ♪ ♫♫♩ ♪♩ ♫𝅝 ♩♪ 𝅝𝅝𝅝♩".

A family of parameters can be associated to each graphical sentence : the number of occurrences of each letter, the number of words, of loops, of arrows, etc.

THE CLASSROOM ACTIVITY. After introducing the above kinds of graphical sentences, the teacher can then ask the following question :

Q : *How many graphical sentences of kind* $\underset{\rightarrow}{\mathscr{L}}^{\circlearrowright}$ *contain exactly* 5 *arrows,* 3 *loops,* 5 *times letter A,* 4 *times letter C,* 5 *times letter G and* 6 *times letter T and no other letter* **?**

• STEP 1. In order to take into account the values of these parameters in a compact way, suggest the student to give a *weight* to each graphical sentence in the form of a monomial in the symbolic variables " $\uparrow$ ", $\circlearrowright$", and each letter "a" of alphabet $\mathbb{A}$. The weight $\mathbf{w}s$ of the following graphical sentence s of kind $\underset{\rightarrow}{\mathscr{L}}^{\circlearrowright}$



would be

$$\text{weight}(s) = \mathbf{w}s = \uparrow^5 \circlearrowright^3 A^5 C^4 G^5 T^6 \tag{1}$$

where the exponent of each symbolic variable is the number of occurrences it appears in s (exponent 0 means that the corresponding item does not appear in s). Of course, the weight of a graphical sentence of kinds $\underset{\rightarrow}{\mathscr{L}}$ and $\underset{\rightleftarrows}{\mathscr{L}}$ will never contain the variable "$\circlearrowright$".

• STEP 2. Define the weight $\mathbf{w}\mathscr{K}$ (or inventory) of any kind $\mathscr{K}$ of graphical sentences as the formal sum of weight of its elements:

$$\text{inventory}(\mathscr{K}) = \mathbf{w}\mathscr{K} = \sum_{s \in \mathscr{K}} \mathbf{w}s \tag{2}$$

and convice the students that the answer to question **Q** is the coefficient of monomial (1) after collecting similar terms in the inventory $\mathbf{w}\underset{\rightarrow}{\mathscr{L}}^{\circlearrowright}$ of the kind $\underset{\rightarrow}{\mathscr{L}}^{\circlearrowright}$ of graphical sentences.

• STEP 3. Help students to find closed forms for the inventories $\mathbf{w}\underset{\rightarrow}{\mathscr{L}}$ and $\mathbf{w}\underset{\rightarrow}{\mathscr{L}}^{\circlearrowright}$ by making use, among other things, of the geometric series

$$\frac{1}{1-X} = 1 + X + X^2 + X^3 + \cdots ,$$

and suggest to use the CA system to answer question **Q**. Of course, when using the CA system, it is more convenient to use other symbols for the variables : for example, α instead of $\uparrow$, λ instead of $\circlearrowright$ and $a_1, a_2, \ldots, a_n$ for the letters of alphabet $\mathbb{A}$.

• STEP 4. The teacher goes one step further by challenging students to compute the inventories of the kinds $\underset{\rightleftarrows}{\mathscr{L}}$ and $\underset{\rightleftarrows}{\mathscr{L}}^{\circlearrowright}$ of *two-way linear graphical sentences.* The extra difficulty is to be careful to "count" only once those kind of graphical sentences having a 180° symmetry.

• STEP 5. Manipulate inventories (by assigning values to variables, making some variables equal, differentiating with respect to some variables, etc) in order to extract more information on the kind of graphical sentences under study.

By the above activity, the students will learn the following facts :

• Geometric (and power) series do not need to be convergent in order to be useful.
• Any symbol can be interpreted as an algebraic variable in concrete situations.
• Monomials can help in making various kinds of "inventories" in classes of objects.
• Manipulation of inventories give much information on various kinds of objects.
• Computer algebra can be of great help even in "simple" enumerative questions.

Keywords
Graphs, sentences, graphical sentences, generating functions

References
[1] G. LABELLE; L. LAFOREST, A Combinatorial Analysis of Tree-Like Sentences. *Open Journal of Discrete Mathematics* **volume**(5), 32–53 (2015).

Gaussian Elimination with Parameters

Aharon Naiman[1] [naiman@jct.ac.il]

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

Basic mathematics courses, at all levels, involve *many* opportunities to include CAS packages. Such systems assist with the preparation of:

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

In this talk we discuss an aspect which affects all of the areas above, i.e., that of solving Gaussian elimination with parameters, in particular for the teaching of basic, first-semester linear algebra.

Right from the beginning of the semester, students are shown how to perform row reduction. As we know, they need to show that there are either no solutions, one unique solution (and what it is), or an infinite number of solutions (and what they are). Are the standard functions of the available packages prepared to show these three possibilities?

The linear systems are then "complicated" by including input parameters. The students need to continue to solve these systems, and specify, based on the input parameters, which of the three possibilites above pertains. Again, do the standard, available functions supply all of the necessary solutions? As we shall show, not all solutions and special cases are covered.

Three approaches are presented using *Mathematica* [2], including one which gets back to basic, row reduction. This last one is particularly useful, as it does all of the calculations itself (à la Computer-Based Maths [1]), step-by-step, so the student misses nothing, and is nonetheless not bogged down with a myriad of arithmetic calculations. This leaves more time for *understanding* the matrix (or individual vectors), as well as applications of solutions of linear systems.

We compare the approaches, demonstrating that some have more satisfying results than others, handling all special cases (and *not* unnecessary ones). We show that one of the approaches delays the need for handling special cases of parameter values along the way, obviating the need for students to recall these special cases until the end.

We end off with applying a final approach to most of the exercises posed in the remainder of the linear algebra course.

Keywords
linear algebra; education; automated Gaussian elimination with parameters; *Mathematica*

References

[1] *Computer-Based Maths* at `computerbasedmath.org`

[2] *Mathematica* at `www.wolfram.com/mathematica`

Proving and Disproving Subspaces with *Mathematica*

Aharon Naiman[1] [naiman@jct.ac.il]

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

Starting from the beginning of one's linear algebra education, one ventures into the area of vector spaces. After learning about the 10 axioms necessary for a vector space, the student delves into subspaces.

As a subspace is also a vector space, we know that we can go back to demonstrating that the 10 axioms are satisfied. However, there is a theorem that states that for a non-empty subset of a vector space, if the subset is closed under vector addition and scalar multiplication, then it is a subspace (and therefore also a vector space itself).

We present what tools are available to us in *Mathematica* [1], to assist in proving or disproving, in familiar mathematical notation, whether a subset is a subspace. First, we need to be able to model a vector space, where the vector subset resides. We demonstrate that we cannot do this, for all trivial vector spaces studied in an elementary course (e.g., function spaces).

Once we have the vector space, we present the necessary functions, together with their many options, to assist in proving that a subset:

1. is indeed a subspace—and *why*, i.e., the relationships of the results of the vector additions and scalar multiplications, or alternatively,
2. is *not* a subspace, and use additional forms of the available functions to demonstrate *intuitive* counterexamples.

For the students, the relationships of the results and the counterexamples are particularly important, in order to impart an instinctive understanding of the material. We further this understanding with some examples of demonstrating all 10 axioms to be fulfilled (or when some are not).

We develop proofs in both directions, using a few, different types of vector spaces, as well as various operations of vector addition and scalar multiplication.

Keywords
linear algebra; education; proving and disproving subspaces; *Mathematica*

References
[1] *Mathematica* at `www.wolfram.com/mathematica`

Teaching Decision Analysis using a Computer Algebra System

Karsten Schmidt[1] [kschmidt@hs-sm.de]

[1] Schmalkalden University of Applied Sciences, Germany

In the Faculty of Business and Economics at Schmalkalden University, the Decision Analysis course in the bachelor program is routinely taught in a traditional classroom setting (blackboard, overhead projector, and pocket calculators). This course is actually one half of the subject “Mathematics II”, the other half is Matrix Algebra, which has been taught in the PC lab for many years (one or two students in front of a PC, instructor’s PC connected to a projector). As the teacher of the Decision Analysis course is currently on maternity leave, I took over teaching of this course for two years from her.

I was curious if topics from the Matrix Algebra portion of “Mathematics II” were useful in the Decision Analysis portion. Particularly as in decision analysis a large number of matrices (sometimes called tables) is used, for example payoff matrices, results matrices, harm matrices, opportunity costs matrices. However, the answer is No.

Nevertheless, having a Computer Algebra System (CAS) readily available is not only useful for matrix operations, but also for finding the perfect alternative, or action, in a decision problem, using other mathematical methods. The usefulness of a CAS in decision analysis will be demonstrated in several examples from different areas, e.g. decisions under certainty, decisions under uncertainty, and decisions under risk.

As the students learn to work with the CAS in the matrix algebra portion anyway, using it (together with a spreadsheet program) also in the decision analysis portion comes without a steep learning curve. Note that students can install the CAS legally on their private PCs as long as they are enrolled in our faculty, and have access to it during the final exam in the PC lab (then, naturally, only one student per PC).

Methodological issues of application of computer algebra in blended learning environment

Daniela Georgieva [1] **, *Elena Varbanova*** [1] [elvar@yu-sofia.bg]

[1] Faculty of Applied Mathematics and Informatics, Technical University of Sofia, Sofia, Bulgaria

We like technology for the sake of our students: it allows to transfer our knowledge and experience to them using tools and environments they are familiar with. In the application of CAS throughout the Teaching-Learning-Assessment (TLA) process our main concern is to develop methodology for technology supported mathematics education [1].

It is well-known that over the centuries unique values and educational tradition have been created. We try to give contemporary/modern interpretation of the educational tradition in the country having in mind purposeful applications of CAS towards the course content, course structure, assessment model and assessment activities. The assessment activities imply the learning outcomes. Being aware of the interrelationship between the teaching, learning and assessment we design and develop teaching and learning materials based on the assessment activities. As a result we change iteratively all the three components of the TLA process. The final goal is the students to build up habits that will be later transformed into educational values.

As we teach undergraduate mathematics (subjects like Engineering Mathematics, Calculus and Numerical methods), examples of methodological approaches to selected topics will be illustrated. The aim is to help students use prototypes, reflect on the results, understand concepts, use their imagination, work smarter not harder, master competencies [2], etc. For this purpose CAS is irreplaceable.

The ACA conferences are a kind of school for exiting and valuable collaborative work. Through any personal experience we all find out that teaching with CAS/technology is just like learning a foreign language: there is a beginning, but no end.

Keywords
Methodology, Computer algebra systems, Teaching-learning-assessment process

References

[1] E. VARBANOVA, About Balanced Application of CAS in Undergraduate Mathematics. In *Applications of Computer Algebra, Springer Proceedings in Mathematics and Statistics*, Springer International Publishing AG 2017, 198, 2017.
[2] E. SHOIKOVA, *Competency Based Education Development: Framework to Plan, Design and Implement Innovative CBE Programs.* Publ. House UNIBIT, Sofia, 2017.

GeoGebra Automated Reasoning Tools:
a problem from Spanish Civil Service Math Teachers' examination

***Zoltán Kovács*[1] , *Tomás Recio*[2] , <u>*M. Pilar Vélez*</u>[3]** [pvelez@nebrija.es]

[1]The Private University College of Education of the Diocese of Linz, Austria
[2] Universidad de Cantabria, Santander, Spain
[3] Universidad Antonio de Nebrija, Madrid, Spain

GeoGebra is open source software, freely available for non-commercial users. It is dynamic mathematics software that brings together geometry, algebra, spreadsheets, graphing, statistics and calculus in one easy-to-use package, for all levels of education.

In 2013, Bernard Parisse's software Giac† was integrated into GeoGebra's Computer Algebra System view. This allowed to include some automated reasoning tools (ART) in GeoGebra, for mechanically finding relations among geometric elements, for testing the truth or falsity of some statement, for finding additional hypotheses for a given statement to hold, cf. [1], [2]. The algorithms behind these tools are based in computational algebraic geometry, cf. [3].

On the other hand, the Spanish recruitment method to become a civil servant math teacher for the secondary school system requires passing and getting the best grades on a series of exams ("oposiciones"). In one of these recent tests, the candidates were requested to solve an elementary geometry question, asking to conjecture, formulate and, then, to prove, the ratio holding between two particular segments in a given figure (see Fig. 1).

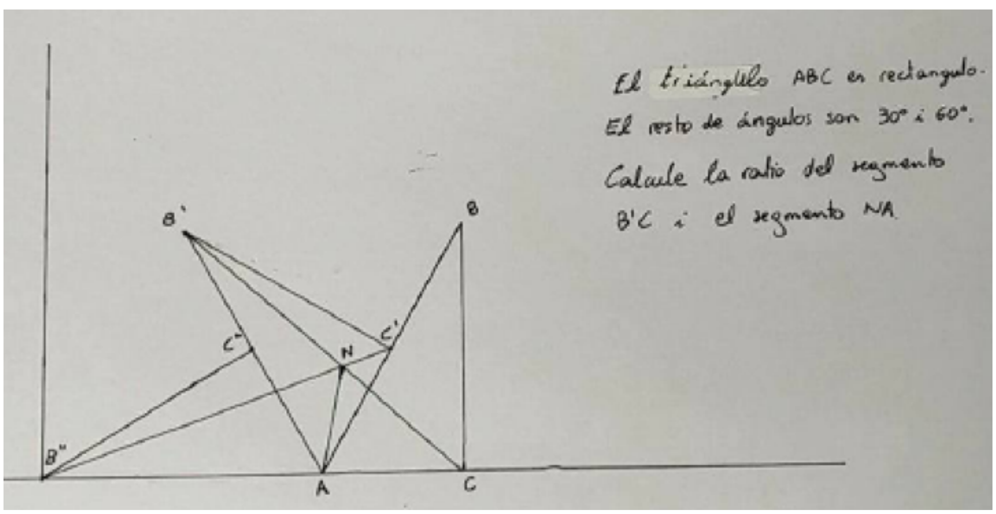


Figure 1: Geometric question from a recent Spanish Math Teachers' recruitment examination: *Triangle ABC is right-angled. The rest of the angles are* 30^o *and* 60^o. *Find the ratio between segment $B'C$ and NA*

†`https://www-fourier.ujf-grenoble.fr/~parisse/giac.htm`

We used GeoGebra ART to accomplish this task, showing, on the one hand, how much it simplifies solving the posed problem; and, on the other, the relevance to adapt and simplify our algorithmic formulation based in elimination ideals [3], to the special zero-dimensional case.

In fact, this example shows that some quite natural, human interpretations of the given situation could lead to a complicated "truth on parts" conclusion (cf. [4]), in which the thesis will simultaneously hold and fail over some irreducible components of the algebraic variety describing the set of instances verifying the hypotheses.

This will imply, in particular, the need to optimize, for the zero dimensional case, the formulation of the algorithms for detecting "truth on parts", thus warning the user about some hidden, unexpected problem that requires further analysis from his/her side.

Our talk with address both the issues related to the mathematical improvements of the automated reasoning algorithms that this example has suggested, as well as the analysis of the desirable interrelation human/machine that could be behind a future scenario towards improving the chances of "passing" the "oposiciones" examination.

Keywords
Dynamic Geometry, Automated Reasoning, GeoGebra

References

[1] M.A. Abánades, F. Botana, Z. Kovács, T. Recio, C. Sólyom-Gecse, Development of automatic reasoning tools in GeoGebra. *ACM Communications in Computer Algebra* **50**(30), 85–88 (2016).
[2] Z. Kovács, T. Recio, 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).
[3] T. Recio, M. P. Vélez, Automatic discovery of theorems in elementary geometry. *Revista Matemática Complutense* **23**, 63–82 (1999).
[4] Z. Kovács, T. Recio, M. P. Vélez, Detecting truth, just on parts. *Revista Matemática Complutense*, `https://doi.org/10.1007/s13163-018-0286-1` (2018).

Boosting Rocket Performance without Calculus

Michael Xue[1] [mxue@vroomlab.com]

[1] Vroom Laboratory for Advanced Computing, Indianapolis, USA

The stages of a two-stage rocket have initial masses m_1 and m_2 respectively and carry a payload of mass P. Both stages have equal structure factors e and equal relative exhaust speed c. The rocket mass, $m_1 + m_2$ is fixed and $\frac{P}{m_1+m_2} = b$.

According to multi-stage rocket's flight equation [2], the final speed of a two-stage rocket is

$$v = -c\log\left(1 - \frac{em_1}{m_1 + m_2 + P}\right) - c\log\left(1 - \frac{em_2}{m_2 + P}\right). \tag{1}$$

Let $a = \frac{m_1}{m_2}$, (1) becomes

$$v = -c\log\left(1 - \frac{ea}{a + 1 + b(a+1)}\right) - c\log\left(1 - \frac{e}{1 + b(a+1)}\right) \tag{2}$$

where $a > 0, b > 0, c > 0, 0 < e < 1$. We will maximize v with an appropriate choice of a.

The above rocket performance optimization problem is solved using calculus [1]. However, there is an alternative that requires only high school mathematics with the help of a Computer Algebra System (CAS). We reduce (2) successively to a new optimization problem where the target function is quadratic. The reduced problem is then solved analytically using high school level algebra (quadratic equation and inequality). This non-calculus approach places more emphasis on problem solving through mathematical thinking, as all symbolic calculations are carried out by the CAS [3]. It also makes a range of interesting problems readily tackled with minimum mathematical prerequisites.

Keywords
Optimization, Computer Algebra, High School Mathematics

References

[1] D. BURGHES; M. BORRIE, *Modelling with Differential Equations*. Ellis Horwood Limited, Chichester, 1982.

[2] M. XUE, *Viva Rocketry!*, at http://vroomlab.wordpress.com/2019/01/31/viva-rocketry-part-2-2.

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

Analysis and modeling of contact stresses between two deformable bodies

Ali Bilek[1]***, Mustapha Beldi***[1]***,***
Said Djebali[1]***, Salah Zouaoui***[1] [alibilek2000@yahoo.fr]

[1] L.M.S.E. Laboratory, Mechanical Engineering Department, UMMTO University, 15000 Tizi-Ouzou, Algeria

This paper deals with a contact problem between two elastic deformable bodies. This kind of problem can be encountered in mechanical systems where contact between moving components can give rise to high stresses, particularly in the neighborhood of the contact zones. To improve design and durability one should determine accurately the type and the amplitude of the imposed stresses. Experimental as well as numerical solutions are used by various authors to tackle this kind of problem [1-3]. The analyzed model consists of a birefringent deformable disc loaded along its diameter by a birefringent deformable plan. The two stress fields developed in the neighborhood of the contact zones are analyzed experimentally with plan polarized light and circularly polarized light in order to obtain respectively the isoclinic fringe pattern and the isochromatic fringe pattern which allow the determination of the stress fields; the principal stresses directions and the values of the principal stresses differences were then easily determined. We used *castem package* to obtain numerically the photoelastic fringes in order to compare them with the experimental ones. Good agreements were achieved. Analysis of stresses along the axis of symmetry showed good agreements between the experimental values and the simulated ones.

Keywords
Stress, Contact, Isochromatic fringes, Isoclinic fringes

References

[1] RABAH HACIANE, ALI BILEK, SAID LARBI, DJEBALI SAID, Photoelastic and numerical analysis of a sphere/plan contact problem. In *Procedia Engineering*, 277–283. 2015.
[2] SOHOULI, A, R., GOUDARZI, A, M., ALASHTI, R, A., Finite Element Analysis of Elastic-Plastic Contact Mechanic Considering the Effect of Contact Geometry and Material Propertie. *Journal of Surface Engineered Materials and Advanced Technology* **1**(3), 125–129 (2011).
[3] MIJOVICAND, B., DZOCLO, M., Numerical contact of a Hertz contact between two elastic solids. *Engineering Modeling* **3**(3-4), 111–117 (2000).

Viscous fingering in five-spot immiscible displacement

Ali Bilek[1] **,** ***Hassane Djebouri***[1] **,**
Kamal Mohammedi[2] **,** ***Salah Zouaoui***[1] `[djebourihassane@gmail.com]`

[1] L.M.S.E. Laboratory, Mechanical Engineering Department, UMMTO University, 15000 Tizi-Ouzou, Algeria
[2] Materials, Processes and Environment Research Unit (URMPE), FSI, M'hamed Bougara University of Boumerdes, Algeria

During immiscible flows in a porous medium, instability, called viscous fingering, can occur at the interface of the two fluids [1,2]. This instability, which has been the subject of much research, occurs in a wide variety of industrial and natural processes, particularly in the enhanced oil recovery where this phenomenon is undesirable because it reduces the sweep efficiency [3]. Faced with a double complexity, that of the nature of the porous medium and that of the nature of the flow, most of the researchers concentrated on simple geometries and on the qualitative aspect of the phenomenon [2]. The work, presented in this paper, is a numerical study that treats the Viscous fingering phenomenon in a five-spot geometry which is considered a good model of the oil fields. The effect of the presence of fractures on the sweep efficiency is considered. The flow equations are solved using the finite volume method (FVM). Brooks-Corey model for relative permeability has been implemented in a finite volume code. The solution method is Implicit in Pressure and Explicit in saturation (IMPES).

Keywords
Porous medium, Fracture, Multiphase flow, Finite Volume Method, IMPES.

References

[1] Farajzadeh, R and Eftekhari, AA and Hajibeygi, H and Kahrobaei, S and Van der Meer, JM and Vincent-Bonnieu, S and Rossen, WR, Simulation of instabilities and fingering in surfactant alternating gas (SAG) foam enhanced oil recovery. *Journal of Natural Gas Science and Engineering* **34**, 1191–1204 (2016).
[2] Islam, MN and Azaiez, J, Thermo-viscous fingering in quarter five-spot miscible displacements. *European Journal of Mechanics-B/Fluids* **30**(1), 107–119 (2011).
[3] Arabloo, Milad and Shokrollahi, Amin and Ghazanfari, Mohammad H and Rashtchian, Davood, Characterization of viscous fingering during displacements of low tension natural surfactant in fractured multi-layered heavy oil systems. *Chemical Engineering Research and Design* **96**, 23–34 (2015).

Pre-Manufacturing Behavior Forecasting and Modeling of Silicon Photonics Dual-Mode Devices Using Computer Algebra

Avi Karsenty[1] [karsenty@jct.ac.il]

[1] Advanced Laboratory of Electro-Optics (ALEO), Applied Physics/Electro-Optics Engineering Department, Lev Academic Center, Jerusalem, Israel

Silicon-based light-emitting devices are extremely desirable for integrating optical signal processing with electronic data processing. These dual-mode devices are basic to develop a generation of ultrafast computers, based on combined electronic and optical signal processing on the one hand, and advanced generations of optoelectronic devices for optical communication systems on the other hand. As part of the efforts to address the need of developing such ultra-fast electro-optics dual-mode processing computers, there is a need to develop an entire family of new silicon-based nanoscale electro-optical components which may smoothly integrate into the existing microelectronics industry. Series of such electro-optics silicon-based devices (transistors, capacitors, photo-activated and thermo-activated modulators, sensors, waveguides...), which optimally couple electrical and optical properties have been developed [1]. Due to the fabrication high-cost of such complex devices, there is a strong need to accurately simulate and forecast their expected electro-optical behavior, using advanced simulations, to assure smooth functionality. Comsol Multi-Physics Package software [2] is employed and integrated with Matlab-Simulink [3]. The physical equations are discretized on a mesh using the Galerkin Finite Element Method (FEM) [4], and to a reduced extent the method of Finite Volumes (FVM). Equations can be implemented in a variety of forms such as directly as a PDE, or as variation integral, the so called weak form [5]. Boundary conditions may also be directly imposed or using variation constraint and reaction forces. Both choices have implication for convergence and physicality of the solution. The mesh is assembled from triangular or quadrilateral elements in two-dimensions, and hexahedral or prismatic elements in three dimensions, using a variety of algorithms, pending the needs. Solution is achieved using direct or iterative linear solvers and non-linear solvers. The former are based on conjugate gradients, the latter generally on Newton-Raphson iterations. The research presents next simulation challenges.

Keywords

Finite Element Method (FEM), Finite Volumes Method (FVM), Partial Differential Equation (PDE), Nanoscale Body Devices (NSB), Simulations, Nanotechnology

References

[1] Advanced Laboratory of Electro-Optics (ALEO) website, https://www.aleo.solutions/.

[2] Comsol Multi-Physics Package SW website, https://www.comsol.com/.

[3] Matlab website, https://www.mathworks.com/products/matlab.html.

[4] G. Strang; G. J. Fix, An Analysis of the Finite Element Method. In *Wellesley-Cambridge Presse*, 2nd edition, Wellesley, 2008.

[5] A. KARSENTY; Y. MANDELBAUM, Computer Algebra Challenges in Nanotechnology: Accurate Modeling of nanoscale electro-optic devices using Finite Elements Method. In *Mathematics in Computer Science (2018)*, pp. 1-14, 06 Aug. 2018.

Reparameterizations and Lagrange piecewise-cubics for fitting reduced data

Ryszard Kozera*[1,2,3]*, Lyle Noakes*[2]*,
***Magdalena Wilkołazka*[3]** [ryszard.kozera@gmail.com]

[1] Faculty of Applied Informatics and Mathematics, Warsaw University of Life Sciences - SGGW, Warsaw, Poland
[2] School of Physics, Mathematics and Computing, The University of Western Australia, Perth, Australia
[3] Faculty of Mathematics, Informatics and Landscape Architecture, The John Paul II Catholic University of Lublin, Lublin, Poland

The problem of estimating the unknown regular curve $\gamma : [0,T] \to \mathbb{E}^n$ from the so-called *reduced data* Q_m has been so far extensively studied in the related literature (see e.g. [1], [3] or [4]). In this setting, Q_m forms the collection of $m+1$ points $Q_m = \{q_i\}_{i=0}^m$ in arbitrary Euclidean space $\mathbb{E}^n$ satisfying the corresponding interpolation conditions $q_i = \gamma(t_i)$. Having selected a specific scheme $\hat{\gamma}$ to fit Q_m (see e.g. [1]), the unknown interpolation knots $\mathscr{T}_m = \{t_i\}_{i=0}^m$ obeying $t_i < t_{i+1}$ must be somehow compensated by their "estimates" $\hat{\mathscr{T}}_m = \{\hat{t}_i\}_{i=0}^m$ subject to $\hat{t}_i < \hat{t}_{i+1}$. Given Q_m, the appropriate choice of $\hat{\mathscr{T}}_m$ should guarantee potentially a fast convergence rate α in estimating γ by $\hat{\gamma}$ at best matching the underlying asymptotics in $\gamma \approx \hat{\gamma}$ as if the missing knots $\mathscr{T}$ were used. A possible recipe for $\hat{\mathscr{T}}_m \approx \mathscr{T}$ is to apply the so-called *exponential parameterization* $\hat{\mathscr{T}}_m^\lambda = \{\hat{t}_{i,\lambda}\}_{i=0}^m$ controlled by Q_m and a single parameter $\lambda \in [0,1]$ - see e.g. [3]. A special case of $\lambda = 1$ yields a well-known *cumulative chord parameteriztion* discussed e.g. in [2], [3], [4] or [11]. The asymptotics in approximating γ by various $\hat{\gamma}$ based on $(Q_m, \hat{\mathscr{T}}_m^\lambda)$ are studied e.g. in [2], [4], [5], [6] or [7]. In particular, for *a modified Hermite interpolant* $\hat{\gamma} = \hat{\gamma}_H \in C^1$ (see [10]) and for an arbitrary $\gamma \in C^4([0,T])$ the following *sharp* result holds, uniformly over $[0,T]$ (see [4], [7] and [9]):

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

where $\psi : [0,T] \to [0,\hat{T}]$ defined in [7] is implicitly parameterized by λ (here $\hat{T} = \hat{t}_{m,\lambda}$). Here $\delta_m = \min_{i\le 0\le m-1}\{t_{i+1} - t_i\}$. The case of $\lambda \in [0,1)$ requires to assume a thinner class of *more-or-less uniform samplings* (see [6]), whereas $\lambda = 1$ stipulates an admission of more general class of the so-called *admissible samplings* - see [4]. For certain applications ψ should constitute a genuine *reparameterization* (e.g. for length $d(\gamma)$ estimation by $d(\hat{\gamma})$). In other cases the mapping ψ needs to be *a non-injective mapping* (e.g. if extra loops in trajectory of $\hat{\gamma} \circ \psi$ are required). The last issue is recently studied for $\hat{\gamma}^H$ in [10]. An analogous asymptotics to (1) is established for Lagrange piecewise-cubics $\hat{\gamma} = \hat{\gamma}^C \in C^0$ in [4], [8] and [11]. Here the mapping $\psi = \psi^c : [0,T] \to [0,\hat{T}]$, defines similarly a Lagrange piecewise-cubic satisfying $\psi^c(t_i) = \hat{t}_{i,\lambda}$.

In this work we formulate and prove sufficient conditions for ψ^c to yield $\dot{\psi}^c > 0$ for both *sparse and dense* reduced data Q_m. The latter enforces ψ^c to be *a reparameterization.* Geometrical and algebraic insight supported by illustrative visualization is also given with the aid of symbolic computations performed in *Mathematica* [12].

Keywords
Interpolation, Reduced data, Convergence, Sharpness and Parameterization

References

[1] C. de Boor, *A Practical Guide to Spline*. Springer-Verlag, New York Heidelberg Berlin, 1985.
[2] M.S. Floater, Chordal cubic spline interpolation is fourth order accurate. *IMA J. Numer. Anal.* **26**(1), 25–33 (2005).
[3] B.I. Kvasov, *Methods of Shape-Preserving Spline Approximation*. World Scientific Publishing Company, Singapore, 2000.
[4] R. Kozera, Curve modeling via interpolation based on multidimensional reduced data. *Stud. Informatica* **4B**(61), 1–140 (2004).
[5] R. Kozera; L. Noakes, Piecewise-quadratics and ε-uniformly sampled reduced data. *Appl. Math. Inf. Sc.* **10**(1), 33–48 (2016).
[6] R. Kozera; L. Noakes, Piecewise-quadratics and exponential parameterization for reduced data. *Appl. Math. Comp.* **221**, 620–638 (2013).
[7] R. Kozera; L. Noakes, C^1 interpolation with cumulative chord cubics. *Fundam. Inf.* **61**(3-4), 285–301 (2004).
[8] R. Kozera; M. Wilkołazka, Convergence order in trajectory estimation by piecewise-cubics and exponential parameterization. *Math. Model. Anal.* **24**(7), 72–94 (2019).
[9] R. Kozera; M. Wilkołazka, A modified Hermite interpolation with exponential parameterization. *Math. Comput. Sc.*, `https://doi.org/10.1007/s11786-018-0362-4`.
[10] R. Kozera; M. Wilkołazka, A note on modified Hermite interpolation. *Math. Comput. Sc.*, submitted.
[11] L. Noakes; R. Kozera, Cumulative chord piecewise-quadratics and piecewise-cubics. In: R. Klette, R. Kozera, L. Noakes, J. Weickert (eds), Geometric Properties from Incomplete Data, *Computat. Imaging Vision* **31**, 59–75 (2006).
[12] S. Wolfram, *The Mathematica Book*. Wolfram Media, 2003.

Dynamics of a generalized Atwood's machine with three degrees of freedom

Alexander Prokopenya[1] [alexander_prokopenya@sggw.pl]

[1] Department of Applied Informatics, Warsaw University of Life Sciences, Warsaw, Poland

We consider a generalized version of Atwood's machine (see [1]) when two bodies of masses m_1, m_2 ($m_2 \geq m_1$) are attached to opposite ends of a massless inextensible thread wound round two massless frictionless pulleys of negligibly small radius. Two separated pulleys are used to avoid collisions of the bodies. Body m_2 is constrained to move only along a vertical while body m_1 moves like a spherical pendulum of variable length. Such a system has three degrees of freedom and its motion is described by the following differential equations

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

Here r is a length of the thread between pulley and body m_1, φ and θ are the spherical angles, g is a gravitational constant, and parameter $\mu = m_2/m_1$. As there is no torque about the vertical line the system has an integral of motion $p_\varphi = r^2\dot{\theta}\sin^2\varphi/(1+\mu)$ that is determined from the initial conditions.

Note that in case of $p_\theta = 0$ body m_1 oscillates in a vertical plane and we obtain the swinging Atwood machine that was a subject of many papers (see, for example, [2], [3]). It was shown that even small oscillations can modify the system motion significantly and some unexpected kinds of motion such as periodic or quasi-periodic motion can arise.

Here we consider the case $p_\theta \neq 0$ when new kind of motion can arise. For example, there exists a conical motion when $r = r_0$, $\theta = \theta_0$ and $\dot{\varphi} = \omega$ are constants. The corresponding solution of system (1) describes a uniform motion of body m_1 in a horizontal plane on a circular orbit of radius $r_0\sin\theta_0$. Simulation of the system motion shows that small variation of the initial conditions results only in small perturbation of the body m_1 orbit. Doing necessary symbolic calculation and analyzing the Hamiltonian function of the system we prove orbital stability of this solution. All relevant symbolic and numerical calculations and visualization of the results are performed with the computer algebra system Mathematica [4].

Keywords
Atwood's machine, Simulation, Periodic motion, Wolfram Mathematica

References

[1] G. Atwood, *A Treatisa on the Rectilinear Motion and Rotation of Bodies.* Cambridge University Press, 1784.
[2] N.B. Tufillaro, T.A. Abbott, D.J. Griffiths, Swinging Atwood's machine. *Amer. J. Phys.* **52**, 895–903 (1984).
[3] A.N. Prokopenya, Motion of a swinging Atwood's machine: simulation and analysis with Mathematica. *Mathematics in Computer Science* **11**, 417–425 (2017).
[4] S. Wolfram, *An elementary introduction to the Wolfram Language, 2nd ed..* Champaign, IL, USA, Wolfram Media, 2017.

Analytical calculations of secular perturbations of translational-rotational motion of a non-stationary triaxial body in the central field of attraction

Oralkhan Baisbayeva[1]***, Mukhtar Minglibayev***[1]***,***
Alexander Prokopenya[2] [alexander_prokopenya@sggw.pl]

[1]Department on Mechanics, Al-Farabi Kazakh National University, Almaty, Kazakhstan
[2]Warsaw University of Life Sciences - SGGW, Warsaw, Poland

The translational-rotational motion of two non-stationary bodies – a spherical body and a triaxial body is investigated. It is assumed that the initial dynamic shapes of bodies are preserved but their masses and sizes change in time [1], [2]. Besides, the reactive forces and additional torques are assumed to be small and may be neglected. An approximate expression for the force function of the Newtonian interaction accurate up to the second zonal harmonics is accepted. The translational-rotational motion of a triaxial non-stationary body is considered in a relative coordinate system with an origin situated in the center of a non-stationary spherical body. The axes of the own coordinate system of the non-stationary triaxial body are directed along its principle axes of inertia and we assume that in the course of evolution their relative orientation remains unchanged. Rotational motion is described in terms of the Euler variables. The problem is complex because the differential equations of motion are non-autonomous and have no integral. Therefore, the problem is investigated in the framework of the perturbation theory. Equations of motion in osculating analogues of Delaunay-Andoyer elements are derived in [1-5]. The unperturbed translational motion is described by an aperiodic motion on quasiconic section [1]. Unperturbed rotational motion is characterized by the Eulerian motion of non-stationary axisymmetric body [1], [2], [5]. Differential equations of the unperturbed translational-rotational motion are integrated by the Hamilton-Jacobi method. Differential equations of unperturbed translational-rotational motion of a non-stationary triaxial body were derived in Jacobi osculating variables. Equations of perturbed motion in the analogues of Delaunay-Andoyer elements have the canonical form

$$L = \frac{\partial F}{\partial l},\ G = \frac{\partial F}{\partial g},\ H = \frac{\partial F}{\partial h},\ l = -\frac{\partial F}{\partial L},\ g = -\frac{\partial F}{\partial G},\ h = -\frac{\partial F}{\partial H}$$

$$L' = \frac{\partial F'}{\partial l'},\ G' = \frac{\partial F'}{\partial g'},\ H' = \frac{\partial F'}{\partial h'},\ l' = -\frac{\partial F'}{\partial L'},\ g' = -\frac{\partial F'}{\partial G'},\ h' = -\frac{\partial F'}{\partial H'}.$$

The perturbing functions$F$, F' in (1), (2) written in the analogues of Delaunay-Andoyer elements are very complicated and one has to do a lot of symbolic computation to obtain them. Such computation can be performed efficiently with the aid of computer algebra systems. Finally, we obtain analytical expressions for the perturbing functions F, F' in the form

$$F = \frac{1}{\nu^2}\frac{\mu_0^2}{2\mu_0 L^2} + \left\{-\frac{1}{2}bR^2 + \frac{(m_1+m_2)}{m_1 m_2}U_2\right\},$$

$$F' = \frac{1}{2}\left(-\frac{1}{m\chi^2}\left[\frac{G'^2}{A_0} + \frac{A_0 - C_0}{A_0 C_0}L'^2\right]\right) - H_{1pert}^{rot}$$

$$H_{1pert}^{rot} = \frac{1}{2}\left(\frac{B-A}{A^2}\right)\left(G'^2 - L'^2\right)\cos^2 l' - \left\{U_2 - \frac{1}{2}bR^2\right\}$$

$$U_2 = f m_1 \frac{A+B+C-3I}{2R^3}, I = A\alpha^2 + B\beta^2 + C\gamma^2,$$

where f is the gravitational constant, the mass of non-stationary spherical body $m_1 = m_1(t)$ is a given function of time, A, B, C are the principle moments of inertia of non-stationary triaxial body, $A = A(t_0)\nu\chi^2$, $B = B(t_0)\nu\chi^2$, $C = C(t_0)\nu\chi^2$, $\nu = \nu(t)$, $\chi = \chi(t)$ are known dimensionless function of time, I is the moment of inertia of the non-stationary triaxial body relative to the axis given by the vector $\overrightarrow{O_1O_2} = \vec{R}$ connecting centers of mass of two bodies, α, β, γ are cosines of the angles formed by a straight line O_1O_2 with central axes of inertia of the non-stationary triaxial body. The perturbing functions F, F' (see (3)-(5)) are calculated analytically in terms of the Delaunay-Andoyer elements for the first time and may be obtained, in principle, with arbitrary accuracy. The corresponding complete expressions are very cumbersome and we do not show them here. Note that all time-consuming cumbersome analytical calculations are performed with the aid of the computer algebra system Mathematica [6], which has a convenient interface and makes it easy to combine different types of calculations. Further development of this work involves the study of the obtained equations for secular perturbations of translational-rotational motion of a triaxial body of constant dynamic shape and variable size and mass, using various analytical and numerical methods.

Keywords
Translational-rotational motion, Non-stationary triaxial body, Secular perturbations.

References
[1] M.Zh.Minglibayev, *Dinamika gravitiruyushchih tel s peremennymi massami i razmerami. Postupatel'noe i postupatel'no-vrashchatel'noe dvizhenie*. Lambert Academic Publishing, Germany, 2012.
[2] Yu.V. Barkin, V.G.Demin, Postupatel'no-vrashchatel'noe dvizhenie nebesnyh tel . *Itogi nauki i tekhniki AN SSSRl* **T**(20), 115–134 (1982).
[3] S.G. Zhuravlev, *Metod issledovaniya ostrorezonansnyh zadach nebesnoj mekhaniki i kosmodinamiki*. SOLTI, Arhangel'sk, 2002.
[4] A.V. Borisov; I.S.Mamaev, *Dinamika tverdogo tela. Gamil'tonovy metody, integriruemost',haos*.Izhevsk: Institut komp'yuternyh issledovani, Moskva, 2005.
[5]A.P. Markeev, *Teoreticheskaya mekhanika*. NIC "Reularnaya i haoticheskaya dinamika", Moskva-Izhevsk,2007.
[6] A.N. Prokopenya, *Reshenie fizicheskih zadach s ispol'zovaniem sistemy Mathematica*. Izdatel'stvo BGTU, Brest, 2005.

A Study of Sensitivity of Nonlinear Oscillations of a CLD Series Circuit to Parametrization of Tunnel Diode

Haiduke Sarafian [has2@psu.edu]

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

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

Keywords
Tunnel Diode, Electrical Nonlinear Oscillations, Computer Algebra System, Mathematica

References

[1] LEO ESAKI DIODE. https://en.wikipedia.org/wiki/Tunnel_diode.
[2] Mathematica^{TM} (2017) is symbolic computation software, V11.2, Wolfram Research Inc.

A Two-Dimensional Nonlinear Oscillator in a Charged Rectangular Frame

Haiduke Sarafian [has2@psu.edu]

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

Motion characteristics of a point-like charged particle projected within the interior plane of a two dimensional electric field of an uniformly charged square and/or rectangular frame is intuitively unpredictable. This investigation quantifies its kinematics. Two scenarios are considered. First, the charged particle is projected along the frame's planar symmetry axis. Second, it is projected at an arbitrary direction within the frame. In both cases the equations of motion are challenging nonlinear differential equations. Applying Computer Algebra System (CAS), specifically Mathematica [1], equations are solved numerically. The first scenario results weak nonlinear oscillations along the symmetry axis. The second case is conducive to a two dimensional chaotic unpredictable oscillations sensitive to speed and orientation of the initial velocity. For visual comprehension of nonlinear oscillations, we utilize Mathematica's innate animation feature simulating the oscillations.

Keywords
Two-dimensional Nonlinear Oscillator, Computer Algebra System (CAS), Mathematica

References

[1] WOLFRAM, S. (1996) Mathematica Book, 3rd Edition, Cambridge University Press, Cambridge.
[2] SARAFIAN, H. (2017) Legendre Polynomials and Nonlinear Oscillating Point-Like Charged Particle. Journal of Electromagnetic Analysis and Applications, 9, 147-154. `https://doi.or/10.4236/jemaa.2017.911013`.
[3] SARAFIAN, H. (2011) Nonlinear Oscillations of a Magneto Static Spring-Mass. Journal of Electromagnetic Analysis and Applications, (2011), 3, 133-139, `doi:10.4236/jemaa.2011.35022.`
[4] SARAFIAN, H. (2017) 6th International Physics Conference, Athens-Greece, July, 2018.
[5] SARAFIAN, H. (2015) Mathematica Graphics Example Book for Beginners. Scientific Research Publishing, Wuhan.

Producing animations of some physical phenomena with KeTCindy

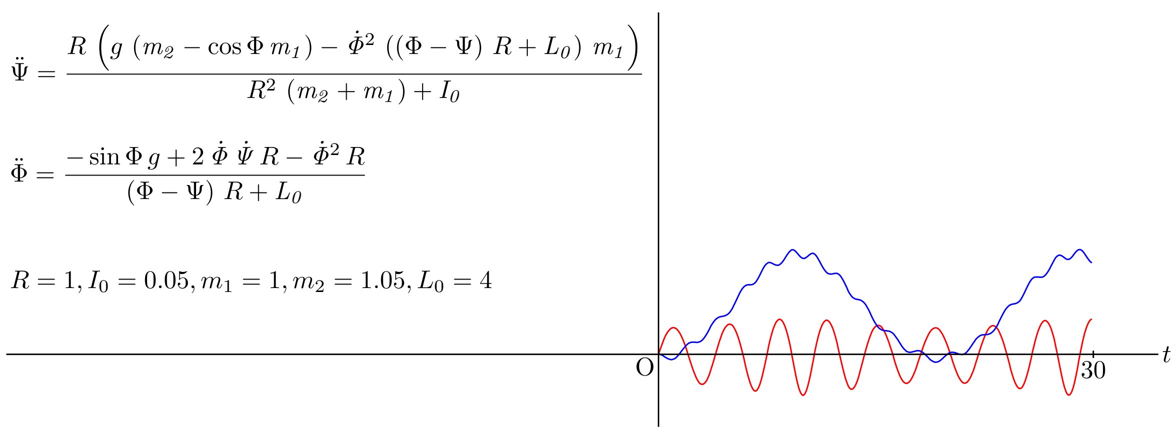
***Alexander N. Prokopenya*[1] , *Setsuo Takato*[2]** [takato@phar.toho-u.ac.jp]

[1] Warsaw University of Life Sciences–SGGW, Poland
[2] Faculty of Science, Toho University, Funabashi, Japan

The first author developed KeTpic to input fine figures easily in the LaTeX document, for example, a printed material to be destributed in Mathematics classes [1]. One can say that it is a kind of preprocessor of graphical codes such as pict2e or Tikz. And now he has developed KeTCindy collaborating with Cinderella, a dynamic geometry software, so as to produce figures interactively and more easily. Anyone can dowload KeTCindy package freely from CTAN(Congressive TeX Archive Network)

`https://ctan.org/pkg/ketcindy.`

Originally, KeTCindy was for Mathematics education and teachers to make their printed materials. But he extended various functions to KeTCindy, so it has become useful also for other fields. An Atwood's machine the second author analysed in [2] may be a good example. The following is a figure produced by KeTCindy.



In our talk, we will show in detail how to draw the figure, how to make calculations, and how to produce the animation. Such animation helps to imagine a real motion of the system and to understand an essence of physical phenomenon.

Keywords
LaTeX, Maxima, KeTCindy, Simulation

References

[1] S. Takato; A. McAndrew; J.A. Vallejo; M. Kaneko, Collaborative use of KeTCindy and free Computer Algebra Systems. *Mathematics in Computer Science* **11**, 503–514 (2017).
[2] A.N. Prokopenya, Motion of a swinging Atwood's machine: simulation and analysis with Mathematica. *Mathematics in Computer Science* **11**, 417–425 (2017).

Graphene transport in a parallel magnetic field: Spin polarization effects at finite temperature

Mircea Crisan [1] **,** ***Ioan Grosu*** [1] **,** ***Ionel Tifrea*** [2] [itifrea@fullerton.edu]

[1] Department of Physics, "Babeş-Bolyai" University, 40084 Cluj-Napoca, Romania
[2] Department of Physics, California State University, Fullerton, CA 92834, USA

We present an analysis of the temperature and magnetic field dependence of the total electron conductivity in monolayer graphene systems due to screening effects around charged impurities [1]. The evaluation of the two spin channels polarization functions and screening coefficients is based on the random phase approximation (RPA) [2]. The total electron conductivity due to both spin-up and spin-down electrons decreases as function of temperature in the low temperature regime, presents a minimum in the intermediate temperature regime, and increases linearly with temperature in the high temperature regime. As function of magnetic field, the system total electron conductivity increases across all temperature regimes. The evaluation of the electron transport functions involves complicated self-consistent calculations that require numerical work. All numerical work was completed using Mathematica.

Keywords
graphene, electron transport, magnetic field

References

[1] T. Ando, Screening Effect and Impurity Scattering in Monolayer Graphene. *J. Phys. Soc. Jpn.* **75**, 074716 (2006).
[2] S. Das Sarma; Shaffique Adam; E. H. Hwang; Enrico Rossi, Electronic transport in two-dimensional graphene. *Rev. Mod. Phys.* **83**, 407–470 (2011).

Mathematical modelling with Fourier series and PDEs

Emmanuel Roque[1] **,** ***Setsuo Takato***[2] **,** ***José A. Vallejo***[1] [jvallejo@fc.uaslp.mx]

[1] Faculty of Science, State University of San Luis Potosí, México
[2] Faculty of Science, Toho University, Japan

Fourier Analysis provides a set of techniques for solving partial differential equations (PDEs) arising in Mathematical Physics, defined over bounded or unbounded domains. In this talk we will present a Maxima package for dealing with PDEs on bounded domains, where separation of variables can be applied. The package is capable of solving the heat, wave and Laplace equations for quite general boundary conditions defined by arbitrary piecewise-continuous functions (this is the kind of condition that guarantees the convergence of the resulting series). Let us stress that the equations are solved symbolically, that is, the complete Fourier series of the solution is computed (of course, the series can be truncated to make numerical computations). As an additional feature, we show how to generate high-quality graphics and animations of the corresponding solutions.

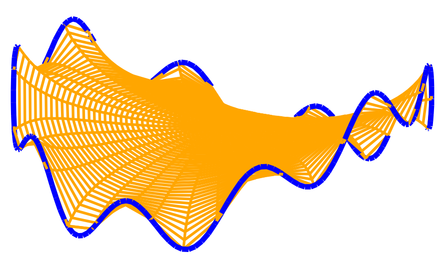


Figure 1: A solution of Laplace equation on the disk with periodic boundary conditions.

We will illustrate the use of the package with several examples of interest in Physics, leaving aside the technical details of the implementation.

Keywords: Fourier Analysis, Partial Differential Equations, Mathematical Software

Towards the numerical simulation of fluid/solid particles flow inside a pipe

Ali Bilek[1] **,** ***Hassane Djebouri***[1] **,** ***Brahim Ferhat***[2] **,**
Kamal Mohammedi[2] **,** ***Salah Zouaoui***[1] [salah.zouaoui@ummto.dz]

[1] L.M.S.E. Laboratory, Mechanical Engineering Department, UMMTO University, 15000 Tizi-Ouzou, Algeria
[2] Materials, Processes and Environment Research Unit (URMPE), FSI, M'hamed Bougara University of Boumerdes, Algeria

The modeling of moving solid particles in fluid flow has been the focus of many studies and has succeeded to attract sufficient attention by researchers. However, commonly used modeling approaches such as discrete element modeling (DEM) and direct numerical simulations (DNS) lack simplicity and have been computationally intensive [1]. The aim of this paper is to develop a new approach to simulate solid transport in an incompressible Newtonian fluid flow. This method is based on the Finite element method with penalization of the deformation tensor [2]. The fluid behavior is governed by the Navier-Stokes equations within the investigation domain. To take into account collisions, we present an algorithm which allows us to handle contacts between rigid particles [3, 4]. In this paper, 2D simulation fluid/particles flow is performed; some preliminary results are presented.

Keywords
Flow, Fluid/Particles, Contact handling

References

[1] Di Renzo A, Di Maio FP., Homogeneous and bubbling fluidization regimes in DEM–CFD simulations: hydrodynamic stability of gas and liquid fluidized beds. *Chem Eng Sci* **62**(1), 116–130 (2007).
[2] Zouaoui S, Djebouri H, Bilek A, Mohammedi K., Modelling and Simulation of Solid Particle Sedimentation in an Incompressible Newtonian Fluid. *Math Comput Sci* **11** (3-4), 527–539 (2017).
[3] Salah Zouaoui, Hassane Djebouri, Ali BILEK and Kamal Mohammedi, Fluid/Particles Flow Simulation by Finite Volume Method -Hybrid Approach-. In *24th Conference on Applications of Computer Algebra ACA2018*, Francisco Botana, Felipe Gago, Manuel Ladra González, 58–61. spublic@usc.es. Santiago de Compostela Spain, June 18-22, 2018.
[4] Maury B., A time-stepping scheme for inelastic collisions. *Numer Math.* **102**(4), 649–679 (2006).

S8 - Proving and Discovery in Geometry

Automated Plane Geometry in Wolfram Mathematica

Peter Barendse[1,2], ***Daniel McDonald***[1] [dmcdonald@wolfram.com]

[1] Wolfram Research Institute, Champaign, Illinois, USA
[2] Department of Materials Science and Engineering, Massachusetts Institute of Technology, Boston, Massachusetts, USA

We discuss new tools in the Wolfram Language (the language of the computing system Mathematica) for automatically drawing as well as making conjectures and proving theorems about symbolically described, coordinate-free scenes in plane geometry. These new functions include `GeometricScene`, `RandomInstance`, `FindGeometricConjectures`, and `FindGeometricProof`, which together support the following workflow.

1. `GeometricScene` allows a user to describe a coordinate-free scene in plane geometry.
2. `RandomInstance` draws a randomized instance of the scene.
3. `FindGeometricConjectures` makes conjectures about the scene.
4. `FindGeometricProof` gives human-readable proofs of theorems that hold given the hypotheses of the scene.

`GeometricScene`, `RandomInstance`, and `FindGeometricConjectures` are currently available in Mathematica Version 12, while `FindGeometricProof` will be introduced in a future version. This talk will address the following aspects of these functions.

1. A `GeometricScene` object contains lists of symbolic point coordinates and scalar parameters, which may or not be assigned numerical values, followed by a list of hypotheses describing a scene involving those points and parameters, with a final optional list of potential conclusions drawn from the hyptheses. The contents of the hypotheses and conclusions must be written within the Wolfram Language framework to be simultaneously general enough to describe any given scene in planar geometry, specifically descriptive enough to allow succinct scene descriptions, and simple enough to be accessible to high school students.
2. `RandomInstance` adds coordinate and parameter values to a `GeometricScene` object by first generating and then nondeterministically solving a constrained optimization problem with those symbolic coordinates and parameters as variables. The `GeometricScene` object stores these values and formats itself as the corresponding graphic.
3. `FindGeometricConjectures` uses the coordinate and parameter values found by `RandomInstance` and stored in a `GeometricScene` object to search for interesting relations that hold in the given instance(s) of the scene.

4. `FindGeometricProof` returns logically sound, human-readable proofs using geometric, not algebraic, reasoning, with redundant or irrelevant steps excised.

`RandomInstance` is an example of a *geometric constraint solver*; for a general discussion of geometric constraint solving, see [2]. `FindGeometricProof` is an example of an *automated theorem prover*; for a general discussion of automated theorem proving in geometry, see [1].

Keywords
geometric constraint solver, automated theorem prover, plane geometry, Euclidean geometry, synthetic geometry

References
[1] J. JIANG; J. ZHANG, A review and prospect of readable machine proofs for geometry theorems. *J Syst Sci Complex* **25**(4), 802–820 (2012).
[2] R. JOAN-ARINYO, Basics on geometric constraint solving. In *Proceedings of 13th Encuentros de Geometrfa Computacional (EGC09)*. Zaragoza, Spain, 2009.

Discovering in DGE — A case study

Jiří Blažek[1] **, *Pavel Pech***[1] [blazej02@pf.jcu.cz]

[1] Faculty of Education, University of South Bohemia, České Budějovice, Czech Republic

The article has a form of a case study. The authors define an open geometrical problem - to determine properties of a third degree's curve [2]. The curve occurs as a locus of foci of conics which are tangent to a given quadrilateral. The problem was solved with the aid of Dynamic Geometry System. At the first stage some facts were discovered experimentally [1]. Subsequently their logical connections were established [3]. The main goal of the article is to highlight the experimental phase, which does not depend on visual perception only, but is illuminated by subject's logic, knowledge and experience. This interweaving (tools of the software and suitable strategy of the subject) has self-strengthening effect enabling to solve tasks, which are out of reach of the subject by classical means.

Keywords
Dynamic geometry, Cubic curves, Experiments in DGE

References

[1] A. Baccaglini-Frank, M. Mariotti, Generating conjectures in dynamic geometry: The maintaining dragging model. *Comput. Math. Learning* **15**, 225–253 (2010).
[2] J. Blažek, P. Pech, On one locus in the plane. *Advances in Intelligent Systems and Computing* **809**, 184–196 (2019).
[3] B. Guven, Using dynamic geometry software to gain insight into a proof. *Int. J. Comput. Math. Learning* **13**, 251–262 (2008).

Investigations with DGS and CAS dealing with problems of equal area and particularly a possible generalization to 3D of the known results of the Lhuillier problem

Jean-Jacques Dahan[1] [jjdahan@wanadoo.fr]

[1] Head of the research group of dynamic geometry, IRES of Toulouse, Paul Sabatier University.

This presentation aims to illustrate the dialectic between DGS and CAS during investigations which goals are to solve geometric problems in 2D, and to reach some possible generalizations in 3D.Some of the problems chosen will show the limits of DGS and CAS in the process of discovery and as well in the process of deductive proof. The problem of cutting a triangle in four equal parts will illustrate perfectly this dialectic. « Constructing from one given point of the plane two triangles of equal areas which bases are two given segments » is a problem that can enhance the use 3D DGS to investigate a possible generalization in3D. Eventually the Lhuillier problem will allow us to investigate in 3D with both CAS and DGS and state that these tools are only tools with their limits (the Lhuillier problem : given a first triangle, where are located points M of the plane which symmetric points with respect to the sides of this triangle define a second triangle with the same area?).

Experiments on isoptics by dynamic coloring

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

A plane curve $\mathscr{C}$ is given. The geometric locus of points in the plane through which passes a pair of tangents making a fixed angle θ is called the θ-isoptics of $\mathscr{C}$. We denote it by $\mathrm{Opt}(\mathscr{C},\theta)$. When $\mathscr{C}$ is strictly convex closed curve, it defines three areas in the plane:

- Through any point inside the curve, no tangent passes.
- Through a point on the curve passes a single tangent.
- Through a point out of the curve passes a pair of tangents.

Isoptics have been studied for conics in [1], [2] (the isoptics of parabolas are arcs of hyperbolas, and the isoptics of ellipses and hyperbolas are described with spiric curves). Isoptics of open rosettes have been studied in [8]. A new approach using a DGS has been presented in [3], enabling to study isoptics of open plane curves. For general open curves, it may happen that certain areas in the plane are isopticless.

In general, if C is a point out of the curve, the closest C is to the curve $\mathscr{C}$, the largest the angle between the tangents. For example, if $\mathscr{C}$ is an ellipse, and if C is inside its director circle, then the angle is obtuse. If C is on the circle, the angle is a right angle. Otherwise, the angle is acute.

We wish to present an experimental approach to the discovery of the various areas in the plane, according to the possible angles between possible tangents. The work is based on a dynamic coloring of the plane using GeoGebra and CindyJS [7].

We begin our investigation by letting $F(x,y)=0$ be the equation of a convex curve. By considering an external point $C(x_C,y_C)$ and the tangents t_A and t_B through it to the curve, we assume that there are two tangents from each point C. The tangent points are respectively $A(x_A,y_A)$ and $B(x_B,y_B)$.

Clearly, the equation of a tangent at the point $P(x,y)$ is of form

$$t_P : F'_x(x,y)\cdot(x-x_C)+F'_y(x,y)\cdot(y-y_C)=0.$$

This can be used to express A and B with the coordinates of C without heavy computer algebra, that is, only by *derivation*, *substitutions* and *numerical equation solving* in one variable, if the following properties hold:

1. F is a polynomial of x and y.
2. F can be written in explicit form, that is, for example as $y=f(x)$.

For instance, when considering the example $F(x,y) = x^2 + 2 - y$, the formula

$$x_{A,B} = \frac{2x_C \pm \sqrt{4x_C^2 - 4y_C + 8}}{2} = x_C \pm \sqrt{x_C^2 - y_C^2 + 2}$$

can be obtained and, from this, we immediately get $y_A = x_A^2 + 2$ and $y_B = y_B^2 + 2$.

Finally, computing $\angle ACB$ is a simple numerical operation that can be performed for each C in the plane, or in a bounding box that corresponds to the user's screen. A possible output is shown in Figure 1 where acute angles are shown in blue and obtuse angles are in red. Right angles will be obtained when the color is black, and this corresponds to the directrix of the parabola. We use a similar technique that is described in [5] and [6]. Our approach, as work-in-progress, can be generalized by embedding a computer algebra system in CindyJS—here we focus on keeping the computations as fast as possible to provide the users with immediate feedback from the computer's side.

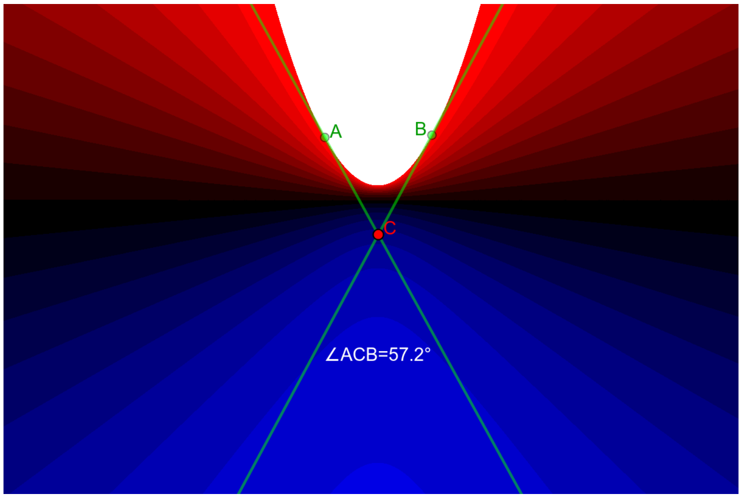


Figure 1: A CindyJS applet that presents the contour plot of isoptic angles of a parabola

Convexity of isoptics has been studied in [6]. As an example, we wish to recall that the isoptics of ellipses are ovals for obtuse angles, and non-convex closed curves for acute angles (see [1]). The same quartics (actually spirics) appear when looking for isoptics of hyperbolas. That time, the isoptic is a union of 4 disjoint arcs on both components of the spiric, as shown in Figure 2 (follow the colors).

A purely algebraic approach is possible from a theoretical point of view: if there exist points of inflexion on the isoptic Opt$(\mathscr{C},\theta)$, then they are points of intersection of $\mathscr{C}$ with its Hessian curve. A CAS may help to compute the solution of the needed system of polynomial equation, but understanding and using the solution on display may be unilluminating. Working with a DGS together with a CAS may contribute to an experimental discovery of points of inflexion.

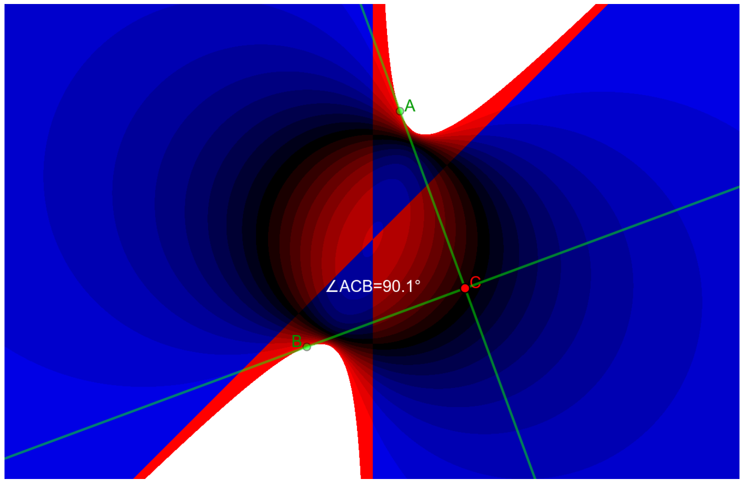


Figure 2: A contour plot of isoptic angles of the hyperbola $F(x,y) = -x^2 + xy - 1 = 0$

Keywords
Isoptics, CindyJS, dynamic coloring

References

[1] TH. DANA-PICARD, G. MANN AND N. ZEHAVI. *From conic intersections to toric intersections: the case of the isoptic curves of an ellipse*, The Montana Mathematical Enthusiast **1**, 59-76 (2011).
[2] 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).
[3] TH. DANA-PICARD AND Z. KOVÁCS. *Automated determination of isoptics with dynamic geometry*, in *Intelligent Computer Mathematics*, F. Rabe, W. Farmer, G. Passmore, A. Youssef (eds.), Lecture Notes in Artificial Intelligence (a subseries of Lecture Notes in Computer Science) 11006, 60-75, Springer (2018).
[4] R. LOSADA. *El color dinámico de GeoGebra*, La Gaceta de la RSME, **17** (3), 525-547 (2014), available: `http://gaceta.rsme.es/abrir.php?id=1220`
[5] R. LOSADA, J. L. VALCARCE AND T. RECIO. *On the automatic discovery of Steiner-Lehmus generalizations*, available: `http://geogebra.es/pub/adg2010def1.pdf`.
[6] A. MIERNOWSKI AND W. MOZGAWA. *On some geometric condition for convexity of isoptics.* Rend. Sem. Mat. Univ. Poi. Torino **55** (2), 93–98 (1997).
[7] A. MONTAG AND J. RICHTER-GEBERT. *Bringing Together Dynamic Geometry Software and the Graphics Processing Unit*, ArXiv , available: `https://arxiv.org/abs/1808.04579`
[8] D. SZALKOWSKI. *Isoptics of open rosettes.* In *Annales Universitatis Maria Curie -Sklodowska Lublin Polonia* LIX, Section A, 119–128 (2005).

The realization of a proof support system in a process of adaptation to the human perspective

<u>*Ludovic Font*</u>[1] , <u>*Philippe R. Richard*</u>[2] , *Sébastien Cyr, Othmane Farid, Michel Gagnon, Fabienne Venant* [ludovic.font@polymtl.ca, philippe.r.richard@umontreal.ca]

[1] Computer Science Department, École Polytechnique de Montréal, Montreal, Canada
[2] Didactic Department, Université de Montréal, Montreal, Canada

1 Context

Although the intelligent tutoring software QED-Tutrix is functional, its successful implementation into the context of a classroom requires an abundant supply of well thought out geometry problems. The goals of this software is to allow teachers to input their own problems in QED-Tutrix and to follow the student's thought process as much as possible while resolving the problem. To decrease the work involved in the complicated task of manually adding a new problem to the software, we developed an automated tool for the generation of mathematical proofs [1]. This automated tool has two main issues. First, the format in which problems are entered requires a reformulation of their typical statement to adapt them to the software's specifications. Second, the proofs obtained by this tool are often very detailed and rigorous due to the generation of every demonstration step, however sometimes obvious for both the teacher and student. Therefore, an improvement in this automated tool must be made for its use in a classroom context. Researchers in the Laboratoire Turing[†] work on two avenues with the goal of adapting the generated proofs: (1) the automated extraction of hypotheses and conclusions from problem statements and (2) the documentation (and later integration into the software) of the different types of referentials used in a class. The first and second avenues are explained in Section 2 and Section 3, respectively.

2 Automated extraction of hypotheses and conclusions from a natural language problem statement

This process is an important addition to the proof generation tool as it will facilitate the task of encoding the problem statement in the QED-Tutrix software. Currently, it is necessary to complete the tedious task of writing down each hypothesis including the low-level ones [2], such as "A is a point" or "there is a line named (AB) passing through A and B", which is especially problematic for busy teachers that would like to quickly add a problem in QED-Tutrix. To automate this process, this information will be extracted directly from the problem statement, written in natural language.

Presently, there are few geometric problem solvers that can automatically extract information from problem statements in their natural language environment [6]. As a result, the understanding and extraction of the hypotheses are delegated to the user who must themselves

[†] http://turing.scedu.umontreal.ca

manually formulate them according to the predefined input interface of the problem solver. This manual extraction might give incorrect results due to a wrong or incomplete interpretation by the user. The major challenge of automatic knowledge extraction is the variation in language. Given a geometry problem statement with a set of fixed hypotheses and conclusions, the extraction can be formulated in several ways without modifying or adding new elements. For example, let us consider these two similar problem statements that might be given in a French-speaking class:

1. "Soit ABCD un quadrilatère quelconque, on appelle P, Q, R et S les milieux respectifs des côtés [AB], [BC], [CD] et [DA]. Montre que le quadrilatère PQRS est un parallélogramme."
   ("Let ABCD be any quadrilateral, we call P, Q, R and S the respective midpoints of the sides [AB], [BC], [CD] and [DA]. Prove that the quadrilateral PQRS is a parallelogram.")

2. "Dans un quadrilatère ABCD, on relie les milieux P, Q, R et S des segments [AB], [BC], [CD] et [DA]. Montre que le quadrilatère PQRS est un parallélogramme."
   ("In a quadrilateral ABCD, the P, Q, R and S midpoints are connected to segments [AB], [BC], [CD] and [DA]. Prove that the quadrilateral PQRS is a parallelogram.")

Each statement contains both the same hypotheses (e.g. "ABCD is a quadrilateral", "P is the midpoint of the line segment [AB]", "Q is the midpoint of the line segment [BC]", "R is the midpoint of the line segment [CD]") and the same conclusion (e.g. "PQRS is a parallelogram"). As depicted in the previous example, other variations in problem statements might be found due to variations in syntax or changes in the order of stated assumptions. Given the potentially very high number of formulations of problem statements, it is important that the automatic extractor should be flexible and have a high tolerance for these linguistic variations.

Another type of variation found in problem statements is the mathematical variation of the hypotheses, where an assumption can be stated in completely different ways while maintaining the same mathematical meaning. For example, the two following assumptions "ABC is a right angle" and "the measure of angle ABC is 90°" are mathematically equivalent, but have been stated in different ways not influenced by linguistic variation. Therefore, the extractor must recognize both these mathematical variations of hypotheses in addition to variations in language. The input states of the problem solvers are finite and limited. Therefore, the extractor must gather equivalent assumptions and place them into equivalence classes, which can be adjusted to these predefined inputs.

3 Documentation of referentials used in class

This task will provide information about which properties are currently used in classrooms. This information will include unusual properties that only a few teachers might use, thereby making the generated proofs feel more natural to the students. In QED-Tutrix, teachers will be capable of dynamically select which properties students can use for a problem at a given time in the school curriculum. The term "referential" is used in the context of the Mathematical Working Space by Kuzniak and Richard [3], where it is the set of properties and definitions used by an individual to solve a problem. We certainly expect this set for a professional mathematician to be bigger than that of an apprentice as it grows as one is learning. The difficulty to document the referentials resides in its dynamic aspect.

In Québec, the ministry is responsible for the curriculum in particular at the high school level (12-17 years old). More specifically, in geometry, the subjects that are to be taught can be summarized by a list of properties. Therefore, there is a first set of sanctioned properties by the ministry, but there is also a second set of suggested properties [4]; thus, we have obligatory and non-obligatory referentials, respectively. This non-obligatory referential is not always used or seen in class, as the referentials in school manuals don't completely match. Although, there is some overlap. At this time, we do not know the exact list used by teachers: is it the one from the ministry, from the school manuals or another personal referential known only by that person? Furthermore, the different properties and definitions are taught in different school years. For example, in Québec, the three cases of similarity of triangles are seen in the fourth year of high school (15-16 years old), the similarity coefficient is seen in the previous third year and the homothety constructions are typically touched in the first or second year [5]. Depending of the school year, students can work with similar concepts, but use different properties.

In these school manuals, we generally find a similar structure in each chapter: exploration activities, class notes, and then exercises. Some also have a referential at the end of the book. As a result, the referential of each chapter precedes the exercises. In some cases, a mathematical problem brings the needs for new properties that are required for its resolution. Similarly, some manuals make the student prove a new property that will be subsequently used in later problems. Therefore, we distinguish two types of referential: (1) the initial referential at the beginning of a chapter and (2) the constructed referential, which contains properties which will be added to a student's referential while they are solving problems. The dynamic nature of the referentials must be considered in the automated solutions of the geometry problems ensuring that QED-Tutrix reflects the reality of what is currently being taught in classrooms.

Keywords
QED-Tutrix, tutoring software, adaptability, automated extraction, referential

References
[1] L. FONT; P. R. RICHARD; M. GAGNON *improving QED-Tutrix by Automating the generation of Proofs.* arXiv preprint arXiv:1803.01468, 2018.
[2] L. FONT *Creation of a Mathematical Model for QED-Tutrix Automated Proof Generator* Presented at the 6th Mathematical Working space symposium in Valparaison, Chile, 2018.
[3] A. KUZNIAK; P. R. RICHARD; Espaces de travail mathématique. Point de vues et perspectives. *Revista latinoamericana de investigación en matemática educativa* **17, 4**(I), 1–37 (2014).

[4] MÉLS *Programme de formation de l'école québécoise premier cycle : Chapitre 6 – Domaine de la mathématique, de la science et de la technologie, 2013.*
Retrieved from `http://www.education.gouv.qc.ca/enseignants/pfeq/secondaire/domaine-de-la-mathematique-de-la-science-et-de-la-technologie/mathematique/`
[5] MÉES *Progression des apprentissages au secondaire. Mathématique, 2016.*
Retrieved from `http://www.education.gouv.qc.ca/enseignants/pfeq/secondaire/domaine-de-la-mathematique-de-la-science-et-de-la-technologie/mathematique/`
[6] M. SEO; H. HAJISHIRZI;A. FARHADI ET AL. *Solving geometry problems: Combining text and diagram interpretation.* Conference on Empirical Methods in Natural Language Processing, 2015.

Rearrangement method for area of a circle: complex paths from historical roots to modern visual and dynamic models in discovery-based teaching approach

Viktor Freiman[1] **, Alexei Volkov**[2] [viktor.freiman@umoncton.ca]

[1] Université de Moncton, NB, Canada
[2] National Tsing-Hua University, Hsinchu, Taiwan

The Internet is full of resources of all kinds (blogs, lesson plans, applets) aiming to introduce the formula for area of circle with 'discovery-based' methods. For instance, [1] suggests considering a circle of radius r as a cake which can be divided in a large number of equal slices (sectors). The slices could then be rearranged pointing alternately up and down to form a shape which looks like a 'rectangle' whose dimensions would be, on one side, radius, and on another side, close to the half of the circumference (which is known as being equal to $2\pi r$), so the area of the 'rectangle' and, therefore, the area of the circle would be $2\pi r^2/2 = \pi r^2$. The author adds that the closeness to 'rectangle' increases when the number of slices increases.

One resource suggested by the NCTM for Grade 7 students presents the same idea as a 'hands-on' activity of cutting (first in 8 sectors, then in 16 sectors) and rearranging the pieces in such a way that students would eventually 'see' a figure originally looking like a parallelogram which is getting closer to the 'rectangle' and then the formula for the circle is obtained from that of the area of the rectangle; see [2]. Using similar ideas, the LearnAlberta provides an interactive animation which allows to increase the number of sides (using a slider), so the rearrangement rapidly approaches the shape of a rectangle, see [3]. A GeoGebra applet created by Ooi Soo Huat, available at [4], allows for some more sophisticated exploration using several sliders to arrive at similar conjectures for the area of the circle.

Old methods of calculation of the area of a circle as applied to the teaching of infinitesimal procedures in the 20th century is an interesting case study within our ongoing project aiming at better understanding of historical roots of didactical approaches [5]. It was widely introduced in many mathematical treatises and textbooks produced since antiquity in East and West to became prominent in Western school textbooks in the second part of the 20th century. In its general form, the procedure can be summarized as follows: the circle is to be subdivided into a large number of identical sectors formed by the radii and the arcs of circumference between their ends. The area of the circle is approximated with the sum of the areas of the triangles having the radii as their long sides. This sum tends to the area of the circle when the number of the triangles grows indefinitely.

Historically, there existed various versions of this procedure slightly different from one another; they will be briefly discussed in our paper. In all the cases the inspected versions of this procedure were based on intuitive understanding of the concept of limit and were not accompanied by rigorous justifications. Similarly, the versions of this procedure found in modern school textbooks did not contain rigorous proofs; instead, they were appealing to the intuition of the learners helping them to 'discover' the formula, both, visually and dynamically.

In this our presentation we will briefly introduce the earliest specimens of this procedure, one found in the commentary of the Chinese mathematician Liu Hui (fl. AD 263) and the other in the manuscripts of Leonardo da Vinci (1452-1519). Then we will pass to the treatment of the area of circle found in West European school textbooks in the late 19th and early 20th century. After that we will investigate who, when, and under what circumstances injected in the school textbooks the method of calculation of area visibly similar to the methods of Liu Hui and Leonardo and discuss the historical background and hypothetical rationale of this didactical innovation. We will conclude the paper with a discussion of the current situation with the use of rearrangement method which can be found in many textbooks produced in a number of countries, as well as in online resources, aiming to a large variety of learners starting from Middle School Grades and towards modern college and undergraduate courses in calculus.

Keywords
Area of circle, Rearrangement formula, History and Modern Teaching

References

[1] T. KÖRNER, What is the Area of a Circle? *Plus+ Magazine*, 2007. `https://plus.maths.org/content/what-area-circle`.
[2] NCTM, Discovering the Area Formula for Circles, `https://www.nctm.org/Classroom-Resources/ARCs/Measures-of-Circles/Circles-Lesson-2/`.
[3] LearnAlberta, Area of the Interior of a Circle, `http://www.learnalberta.ca/content/memg/Division03/Circle/CircleArea/index.html`.
[4] https://www.geogebra.org/m/AADN5Ruq.
[5] A. VOLKOV; V. FREIMAN, Infinitesimal procedures in modern and medieval mathematics textbooks. Paper presented at the annual meeting of the North American Chapter of the International Group for the Psychology of Mathematics Education, TBA, Mérida, Yucatán, Mexico, Nov 09, 2006.

One method of trisecting an angle and its interpretation for teaching purposes using a dynamic geometry and computer algebra system

Roman Hašek [hasek@pf.jcu.cz]

Department of Mathematics, University of South Bohemia in České Budějovice, Faculty of Education, Czech Republic

This contribution is focused on the use of a dynamic geometry and computer algebra system in mathematics education, namely in teaching at secondary schools and in the teaching of future mathematics teachers of lower and upper secondary schools. It presents the use of the software to interpret historical geometrical subject matter from the perspective of up to date mathematics, to create a dynamic model of the respective phenomenon and also to serve as a basis to create its physical model.

The contribution deals with a method of trisecting an angle [5] that was developed by J. R. Vaňaus, Czech mathematician, in his paper *Trisektorie* published in 1881 [7].

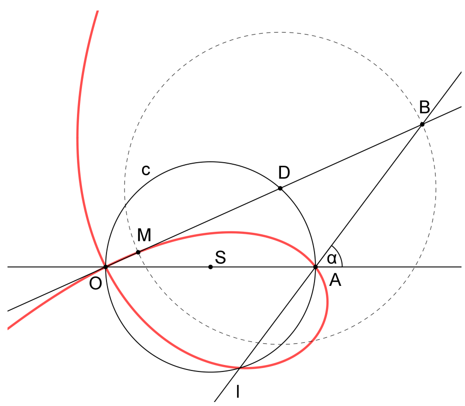


Figure 1: Vaňaus' trisectrix

Let us start the introduction of this method by presenting the example that Vaňaus assigned to readers of the Czech "Journal for doing mathematics and physics" in 1902: *Given a line segment AB. Circular arcs, both with the radius $|AB|$, are drawn around points A and B, passing through points B and A respectively and intersecting at point C. The task is to set points M and N at arcs AC and BC respectively so that the line segment MN is parallel to AB and the angle $\angle MAN$ is equal to a given acute angle.* [8] Three solutions to this problem, all leading to the trisection of an angle, sent by students of upper secondary school, were published in the last issue of the journal volume. In his comment to the solutions Vaňaus mentioned his 1881 paper in which he introduced a method of doing a trisection using the cubic curve shown in Fig. 1.

This cubic curve, currently known as the oblique strophoid [6, 4, 3], is presented by him as the locus of points M for B moving along the line l, a secant to the circle c, so that $|MD| = |DB|$, where D is the intersection of the line SB with c. He derives the equation of this curve and describes a simple way of using it to trisect an angle (the angle α in Fig. 1). In conclusion he mentiones his assembly of a simple mechanism to implement this trisection.

In this contribution we will show the use of the dynamic geometry and computer algebra features of GeoGebra software [2] to create a dynamic model of the respective geometric construction, to derive an equation of the curve and to design a virtual model of the mechanical linkage for the manual execution of the trisection. We will show that supported by the means of the automated theorem proving implemented into the dynamic geometry environment of GeoGebra [1] such tasks are at a corresponding level of complexity already feasible at secondary school.

Keywords
DGS, CAS, trisection, strophoid, mathematics education

References

[1] F. Botana; M. Hohenwarter; P. Janičić; Z. Kovács; I. Petrović; T. Recio and S. Weitzhofer. *Automated Theorem Proving in GeoGebra: Current Achievements*, Journal of Automated Reasoning, 55(1), pp. 39-59 (2015).
[2] *GeoGebra, free mathematics software for learning and teaching*. Available at `http://www.geogebra.org`.
[3] C. G. Gibson. *Elementary Geometry of Algebraic Curves: an Undergraduate Introduction*. Cambridge University Press, Cambridge. 1998.
[4] E. H. Lockwood. *Book of curves* (Reprint). Cambridge University Press, Cambridge. 2007.
[5] A. Ostermann; G. Wanner. *Geometry by its history* [1st ed.]. Springer, Berlin. 2012.
[6] Strophoid (n. d.). In *Wikipedia*. Retrieved April 16, 2019,
from `https://en.wikipedia.org/wiki/Strophoid`.
[7] J. R. Vaňaus. Trisektorie. *Časopis pro pěstování mathematiky a fyziky*. Vol. 10(1881), No. 3, pp. 153–159.
[8] J. R. Vaňaus. Úloha 36. *Časopis pro pěstování mathematiky a fyziky*. Vol. 31(1902), No. 3, p. 262.

Vers un travail géométrique conforme et correct en contexte d'usages d'outils géométriques classiques et numériques

Alain Kuzniak[1] **, Assia Nechache**[2] [alain.kuzniak@univ-paris-diderot.fr]

[1] Département de Mathématiques, Université de Paris, Paris, France
[2] Espé Cergy, Université de Cergy, Cergy, France

1 Objectifs de l'étude

Nos études antérieures [1] sur la résolution de problèmes géométriques par des futurs professeurs de l'enseignement primaire, en France, nous ont permis de dégager une forme de travail géométrique erronée mais très fréquente. Elle se caractérise par le fait qu'elle semble respecter toutes les formes extérieures du processus d'élaboration du travail géométrique mais que le résultat produit n'est pas correct. Le travail géométrique apparaît ainsi à la fois conforme et non correct. Pour paraphraser une publicité ancienne sur une boisson canadienne, le travail géométrique développé présente toute les apparences d'un travail géométrique authentique mais il n'en est pas un. Dans cette communication, nous expliciterons ce point en nous appuyant sur la théorie des Espaces de Travail Mathématique (ETM) qui permet d'évaluer les processus et résultats du travail géométrique réellement produit. Puis, nous explorerons un mode d'entrée dans le travail géométrique basé sur l'usage des outils géométriques et algébriques classiques et digitaux dont nous pensons qu'il est susceptible d'étayer les étudiants en moyens de contrôle sur leurs propres productions. Cette contribution participe du débat sur le rôle et l'utilisation de ces outils dans l'enseignement des mathématiques, et en particulier, sur leur influence potentielle relativement à la preuve et à la démonstration.

2 Un état des lieux: Alphonse ou un travail géométrique hors de contrôle

Dans le cadre du master de formation des maîtres du premier degré en France, nous avons proposé à des étudiants de première année de master une tâche géométrique sur l'estimation de l'aire d'un terrain, "le terrain d'Alphonse".

2.1 La situation d'Alphonse

Dans un premier temps, l'énoncé de la tâche a été distribué sans l'information complémentaire concernant la longueur de l'une des diagonales du terrain et les étudiants ont pu chercher une solution pendant dix minutes. Il est attendu ici qu'ils constatent le manque de certaines données pour pouvoir fixer le quadrilatère et résoudre complétement la tâche.

"Alphonse vient juste de revenir d'un voyage dans le Périgord où il a vu un terrain en forme de quadrilatère qui a intéressé sa famille. Il aimerait estimer son aire. Pour cela, durant son voyage, il a mesuré, successivement, les quatre côtés du champ et il a trouvé, approximativement, 300 m, 900 m, 610 m, 440 m. Il a beaucoup de mal à trouver l'aire. Pouvez-vous l'aider en lui indiquant la méthode à suivre ? "

Pour réaliser cette tâche, les étudiants doivent mobiliser des connaissances portant sur les quadrilatères, la notion d'échelle et l'aire d'un quadrilatère. De manière originale, la réalisation de cette tâche suppose une première modélisation liée à la forme et la représentation du terrain. Cette situation d'enseignement vise à aider les étudiants à identifier les paradigmes géométriques en jeu dans la résolution d'une tâche géométrique de façon à éviter certains blocages et malentendus sur le travail mathématique attendu.

2.2 Quelques conclusions

Contrairement aux attentes initiales, cette phase a suivi un déroulement inattendu du fait que la quasi-totalité des étudiants n'a pas relevé la nécessité d'obtenir des conditions supplémentaires pour fixer la forme du quadrilatère. En effet, les étudiants se sont engagés dans la recherche de l'aire du terrain en ajoutant spontanément certaines conditions supplémentaires (le quadrilatère est nécessairement particulier ou tous les quadrilatères ont la même aire puisqu'ils avaient le même périmètre).

De ce premier constat nous avons pu tirer des conclusions alarmantes sur l'absence de contrôle des étudiants sur leur travail. Ceci étant en grande partie dû au fait que les étudiants ont développé un *référentiel cognitif* en contradiction avec le référentiel théorique standard. Ce *référentiel* s'appuie sur un ensemble de connaissances et d'assertions fausses ou pour le moins discutables:

- Des théorèmes en actes faux (Aire Périmètre):
- L'usage systématique de formules même imaginaires;
- Les figures impliquées dans un problème sont nécessairement des figures particulières.

Ce *référentiel cognitif* provient de la pratique antérieure de la géométrie par les étudiants qui leur permet, dans le meilleur des cas de produire un travail géométrique dont les processus et méthodes paraissent riches et conformes au paradigme dominant mais dont les résultats sont érronés faute d'un contrôle basé sur un référentiel théorique correct.

3 Développer les outils de contrôle dans le cadre d'une géométrie I assumée

3.1 Le travail de Francis comme archetype possible du travail attendu

A partir des résultats de cette première recherche, nous avons décidé de développer le travail géométrique des étudiants sur celui produit par un des leurs, Francis. Ce dernier a effectué une construction de la figure à l'échelle en utilisant une régle et un compas. Par ajustement, il a obtenu un trapèze guidé par l'idée que la figure devait être particulière. En utilisant diverses propriétés géométriques et des constructions imprécises obtenues par ajustement, il a justifié que sa figure était bien un trapèze. Ensuite, il a obtenu l'aire de cette figure en combinant formule et mesure sur le dessin. Il explique qu'il a le droit de faire cela car il a utilisé une échelle pour faire la figure. Son travail semble remplir les attentes de la Géométrie I du point de vue des processus mais les résultats ne sont pas corrects faute de contrôles suffisants. Nous dirons ici que ce travail géométrique est conforme mais non correct. En ce sens, ce travail est plus riche que le celui qui domine chez les étudiants qui était à la fois non conforme au niveau des processus et non correct au niveau des résultats.

3.2 La place spécifique des outils numériques

En nous appuyant sur le travail géomérique produit par Francis, notre objectif est d'amener les étudiants à développer un travail conforme aux règles de la Geométrie I mais aussi correct car contrôlé théoriquement et instrumentalement. Le travail géométrique attendu repose sur la construction des figures avec des outils, une approximation maitrisée de la mesure, un ensemble de procédures de contrôle (triangulation, travail sur les formules). De cette façon, nous pensons destabiliser le référentiel cognitif des étudiants de façon à l'ajuster au référentiel épistémologique attendu à ce niveau.

Pour remettre en question le travail effectué précédemment, nous avons choisi de faire explorer les diverses configurations et formules d'aires possibles en utilisant une version de GeoGebra sur tablette. Pour analyser ce travail, nous utiliserons les différents types de preuves possibles associés aux différents plans verticaux de l'ETM [2]. Il s'agira d'évaluer si cette entrée informatique relativement modeste permet de rendre le travail géométrique des étudiants à la fois complet et conforme lorsqu'ils se retrouvent à nouveau dans un environnement classique du fait de la remise en cause de leur réferentiel cognitif.

Keywords
Didactique, géométrie, travail mathématique

References

[1] A. KUZNIAK; A. NECHACHE, Le terrain d'Alphonse ou les incertitudes de la mesure In *Actes du colloque Copirelem*, Blois, 2018.
[2] P.R. RICHARD; F. VENANT; M. GAGNON, Issues and challenges about instrumental proof. In *Proof Technology in Mathematics Research and Teaching*, Hanna, G., Reid, D., de Villiers. M. (eds). Springer, New-York,2019.

The Modelisation of the Possible Proofs for High School Geometry Problems in the Tutoring Software QED-Tutrix

Ludovic Font*[1] *, Michel Gagnon*[1] *, Nicolas Leduc*[1] *,
***Philippe R. Richard*[2] *, Michèle Tessier-Baillargeon*[2] [nicolas.leduc@polymtl.ca]**

[1] École Polytechnique de Montréal, Montréal, Canada
[2] Université de Montréal, Montréal, Canada

1 Context

The intelligent tutoring system QED-Tutrix [1,2] aims at providing an environment in which a high school student can solve proof problems in geometry, and at helping the student during the whole solving process. This is done thanks to a tutoring engine that reads the interaction between the student and the interface, and then uses that knowledge to infer the proof he seems to be working on, in order to provide him or her with advice to complete his or her proof, if such help is needed.

A crucial part of this engine is a structure in which all the possible proofs (accessible to a high school student) for the problem are stored. This way, it becomes possible to anticipate what the student is likely to attempt to do next, and therefore to help him in a relevant way. In this paper, we present this structure, called the HPDIC graph. Details concerning its functionality are presented in Section 2, and we explain in more depth how the graph is used in QED-Tutrix in Section 3.

2 HPDIC graph representation

To represent a mathematical proof as a computer structure, we must first define precisely what we consider to be a "proof" in the context of high school geometry problem resolution. Our definition, based on the one proposed by Duval [3] is built around the concept of inference. An inference can be seen as an atomic sentence, composed of some premises (ABC is a triangle, and the lengths of line segments [AB] and [AC] are equal), the invocation of a justification in the form of a definition, property or theorem (a triangle with two equal sides is isosceles), and the inferred result (ABC is isosceles). Since the result of an inference can be used as a premise for another, we can build a proof by chaining inferences, starting from the hypotheses of the problem and reaching its conclusion.

The structure of such an inference chain is perfectly suited to be stored in a graph, as has been done in works going as further back as 1984 [4]. Therefore, we define the HPDIC graph (**H**ypotheses, **P**roperties, **D**efinitions, **I**ntermediate results, **C**onclusion) as follows. First, let us consider one proof (i.e., one chain of inferences) for a problem. Each inference is represented by a subgraph: one node for each premise of the inference, one for the justification, and one for the result. These nodes are then linked following two rules : the premises of an inference are linked to the justification representing it, and that justification is linked to its inferred result.

Since the result of an inference can be used as a premise in another one, we merge identical intermediate nodes. These rules create a graph from the hypotheses of the problem to its conclusion. Then, since each proof of a problem uses a subset of the same set of hypotheses, reaches the same conclusion, and uses a subset of the same set of intermediate results, it is possible to put together all the inferences used in **any** proof of a given problem in a graph that we name the HPDIC graph of the problem. This process is illustrated in Figure 1. Figure 1a shows a simple inference. In Figure 1b, this inference (in bold) is used as a step for a complete proof, and, in Figure 1c, this proof (in bold) is merged with another proof, creating the complete HPDIC graph for this fictive problem.

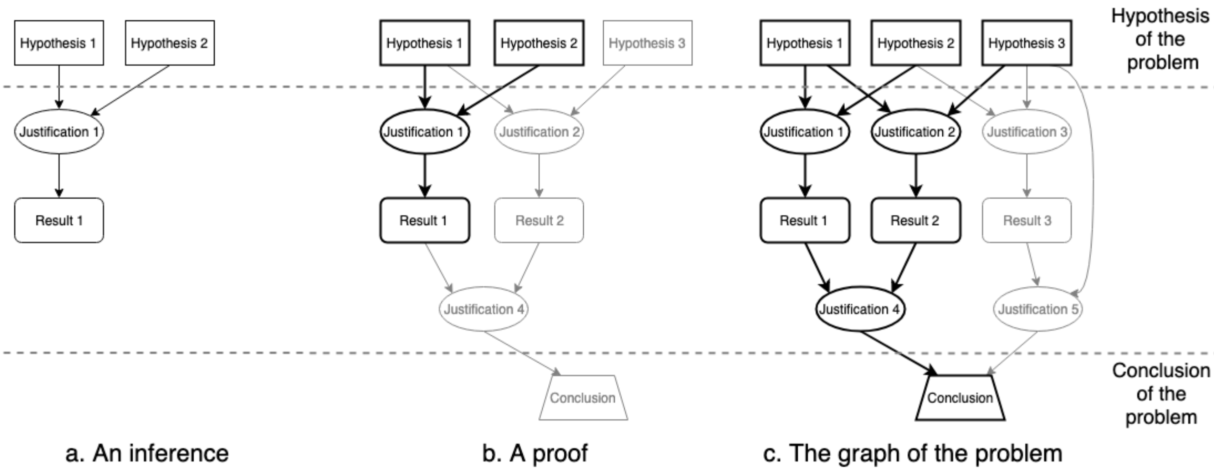


Figure 1: The process of constructing the HPDIC graph

The strength of this representation is twofold. First, it provides a representation of proofs that mirrors the work of high school students. This fundamental requisite is usually not fulfilled by automated theorem proving, since popular methods use intermediate representations, such as the translation of the problem into a system of equations, that is solved by an algorithm [5, 6]. This process provides mathematically valid proofs, but those are also completely out of the scope of high school mathematics education. Furthermore, the broad goal of automated theorem proving is to provide exactly one proof of the theorem, whereas we require the creation of all proofs accessible at a high school level. Second, the structure is very flexible and allows the representation of proofs that use any kind of properties, ranging from small, precise demonstration steps to advanced theorems. This flexibility is crucial when we consider the constant variations in the educational referential. Indeed, the properties that a student is allowed to use change depending on many factors, such as the position in the curriculum, the subject the teacher is emphasizing at the moment, or even the teacher's personal preferences and habits.

3 Uses of the HPDIC graph

During the resolution of a problem by a student in QED-Tutrix, the HPDIC graph is used as a referential to identify the proof that the student seems to be working on. This is done by tagging in the graph each proof element (property or result) entered by the student. Then, an algorithm finds out which proof among all the possible ones is the most advanced, calculated as a percentage of the tagged elements among all the elements used for the proof. This information is recalculated each time the student submits a new element.

Then, using this knowledge, the tutor engine can find out which elements are missing for the student to complete their proof. The tutor is therefore able to guide him/her toward these missing elements. These processes of tagging on the graph and providing messages to help the student are detailed in the work of Nicolas Leduc [1].

In the initial version of QED-Tutrix, the HPDIC graphs were constructed manually by an expert in mathematics education. This process is explained in her work [2]. In particular, the solutions proposed in the HPDIC graph have been validated by several experimentations in class. Five diverse problems were implemented this way, with the aim of encompassing a large number of mathematical concepts, indicating that the HPDIC graph structure is indeed appropriate to represent proofs used in a real classroom context. To improve the scope of QED-Tutrix, we are currently working on a tool to automatically generate the HPDIC graphs for any given problem [7].

Keywords
Proofs, Modelisation, Tutor software

References

[1] N. Leduc, *QED-Tutrix : système tutoriel intelligent pour l'accompagnement d'élèves en situationde résolution de problèmes de démonstration en géométrie plane*. Ph.D. thesis, École polytechnique de Montréal, 2016.
[2] M. Tessier-Baillargeon, *GeoGebraTUTOR : Développement d'un système tutoriel autonome pourl'accompagnement d'élèves en situation de résolution de problèmes de démonstration en géométrie plane etgenèse d'un espace de travail géométrique idoine*. Ph.D. thesis, Université de Montréal, 2015.
[3] R. Duval, *Structure du raisonnement deductif et apprentissage de la demonstration*. Educational Studies in Mathematics, 1991.
[4] D. Gaud; J. P. Guichard, Apprentissage de la démonstration. *Petit x* **vol. 4**, 5–25, 1984.
[5] B. Buchberger, Applications of Gröbner bases in non-linear computational geometry. *Trends in computer algebra*, 52–80, 1988.
[6] H. Wu, An elementary method in the study of nonnegative curvature. *Acta Mathematica* **vol. 142**, 57–78, 1979.
[7] L. Font; P.R. Richard; M. Gagnon, Improving QED-Tutrix by Automating the Generation of Proofs. In *Proceedings 6th International Workshop on Theorem proving components for Educational software, ThEdu@CADE*, Pedro Quaresma and Walther Neuper, 38–58. Gothenburg, Sweden, 2017.

Tracing the Evolution of Current Automatic Proving Technologies

Pedro Quaresma[1] [pedro@mat.uc.pt]

[1] CISUC / Mathematics Department, University of Coimbra, Coimbra, Portugal

Given its formal, logical, and spatial properties, geometry is well suited to teaching environments that include dynamic geometry systems (DGSs), geometry automated theorem provers (GATPs), and repositories of geometric problems. These tools enable students to explore existing knowledge in addition to creating new constructions and testing new conjectures. With the help of a DGS, students can visualise geometric objects and link the formal, axiomatic nature of geometry (e.g., Euclidean geometry) with its standard models and corresponding illustrations (e.g., the Cartesian model). With the help of GATPs, students can check the soundness of a construction (e.g., if two given lines are parallel) and also create formal proofs of geometric conjectures. Supported by repositories of geometric knowledge, these tools provide teachers and students with a framework and a large set of geometric constructions and conjectures for doing experiments.

The evolution of current automatic proving technologies is traced [14]. How these technologies are beginning to be used by geometry practitioners in general to validate geometric conjectures and generate proofs with natural language and visual rendering, and foresee their evolution and applicability in an educational setting. Following Gila Hanna's [5, p.8] argument that "the best proof is one that also helps understand the meaning of the theorem being proved: to see not only that it is true, but also why it is true," and the large number of articles on proof and proving in mathematics education from the ICMI Study 19 Conference [12, 13], the focus must be on practices of verification, explanation, and discovery in the teaching and learning of geometry.

In the classroom, the fundamental question a proof must address is "why?" In this context, then, it is only natural to view proofs first and foremost as explanations and, as a consequence, to give more value to those that provide a better explanation. Dynamic geometry systems encourage both exploration and proof because they make it so easy to pose and test conjectures. The feature that preserves manipulations allows students to explore "visual proofs" of geometric conjectures. Such a powerful feature gives them strong evidence that a theorem is true and reinforces the value of exploration by giving them confidence on the truthfulness of a given geometric property.

The challenge facing classroom teachers is how to use the excitement and enjoyment of exploration to motivate students while also explaining that visual exploration is not a proof. Visual exploration is a useful aid, but is still only the exploration of a finite number of cases. One reason for giving students a formal proof is that exploration does not reflect the need for rigour in mathematics. Indeed, mathematicians aspire to a degree of certainty that can only be achieved by a proof. A second reason is that students should come to understand the first reason. As most mathematics educators would agree, students need to be taught that exploration, useful as it may be in formulating and testing conjectures, does not constitute a proof [5, 6]. A proof is a means of obtaining certainty about the validity of a conjecture (proof as a validation tool) and a strategy to further understand a formulated conjecture (proof as an instrument of understanding).

Geometry automated theorem provers open the possibility of formally validating properties of geometric constructions. For example: *Cinderella*† [16] has a randomised theorem checker; *Java Geometry Expert* (*JGEX*)‡ [20], *Geometry Constructions LaTeX Converter* (*GCLC*)†† [8] and *GeoGebra*‡‡ (version 5) [7] incorporate a number of automated theorem provers that provide a formal answer to a given validation question [2, 10].

Automated deduction techniques also enable students to explore new knowledge and discover new results and theorems [19] (e.g., the algebraic formula of a loci [1, 15]). An important addition to any learning environment would be a GATP with the ability to produce human readable formal proofs with, eventually, visual counterparts [3, 4, 9, 11, 17, 18].

Keywords
Dynamic Geometry, Computer Algebra, Automated Deduction, Computational Tools in Education

References
[1] Miguel Abánades, Francisco Botana, Zoltán Kovács, Tomás Recio, and Csilla Sólyom- Gecse. Towards the automatic discovery of theorems in geogebra. In Gert-Martin Greuel, Thorsten Koch, Peter Paule, and Andrew Sommese, editors, Mathematical Software – ICMS 2016, pages 37–42, Cham, 2016. Springer International Publishing.
[2] Francisco Botana, Markus Hohenwarter, Predrag Janičić, Zoltán Kovács, Ivan Petrović, Tomás Recio, and Simon Weitzhofer. Automated Theorem Proving in GeoGebra: Current Achievements. Journal of Automated Reasoning, 55(1):39–59, 2015.
[3] Shang-Ching Chou, Xiao-Shan Gao, and Jing-Zhong Zhang. Automated generation of readable proofs with geometric invariants, I. multiple and shortest proof generation. Journal of Automated Reasoning, 17(13):325–347, 1996.
[4] Shang-Ching Chou, Xiao-Shan Gao, and Jing-Zhong Zhang. Automated generation of readable proofs with geometric invariants, II. theorem proving with full-angles. Journal of Automated Reasoning, 17(13):349–370, 1996.
[5] Gila Hanna. Proof, explanation and exploration: An overview. Educational Studies in Mathematics, 44(1-2):5–23, 2000.
[6] Gila Hanna and Nathan Sidoli. Visualisation and proof: a brief survey of philosophical perspectives. ZDM, 39(1-2):73–78, 2007.

† https://cinderella.de
‡ http://www.cs.wichita.edu/~ye/
†† http://poincare.matf.bg.ac.rs/~janicic/gclc/
‡‡ https://www.geogebra.org/

[7] M HOHENWARTER. Geogebra - a software system for dynamic geometry and algebra in the plane. Master's thesis, University of Salzburg, Austria, 2002.
[8] PREDRAG JANIˇCI´C. GCLC — A tool for constructive euclidean geometry and more than that. In Andrés Iglesias and Nobuki Takayama, editors, Mathematical Software - ICMS 2006, volume 4151 of Lecture Notes in Computer Science, pages 58–73. Springer, 2006.
[9] PREDRAG JANIˇCI´C, Julien Narboux, and Pedro Quaresma. The Area Method: a recapitulation. Journal of Automated Reasoning, 48(4):489–532, 2012.
[10] PREDRAG JANIˇCI´C AND PEDRO QUARESMA. Automatic verification of regular constructions in dynamic geometry systems. In Francisco Botana and Tomás Recio, editors, Automated Deduction in Geometry, volume 4869 of Lecture Notes in Computer Science, pages 39–51. Springer, 2007.
[11] ZOLTÁN KOVÁCS. Computer based conjectures and proofs in teaching Euclidean geometry. PhD thesis, Universität Linz, 2015.
[12] FOU-LAI LIN, FENG-JUI HSIEH, GILA HANNA, AND MICHAEL DE VILLIERS, editors. Proceedings of the ICMI Study 19 conference: Proof and Proving in Mathematics Education, volume 1. The Department of Mathematics, National Taiwan Normal University, 2009.
[13] FOU-LAI LIN, FENG-JUI HSIEH, GILA HANNA, AND MICHAEL DE VILLIERS, editors. Proceedings of the ICMI Study 19 conference: Proof and Proving in Mathematics Education, volume 2. The Department of Mathematics, National Taiwan Normal University, 2009.
[14] PEDRO QUARESMA AND VANDA SANTOS. Proof Technology in Research and Teaching, chapter Computer-generated Geometry Proofs in a Learning Context. Springer, 2019. (in press).
[15] TOMAS RECIO AND MARÍA P. VÉLEZ. An Introduction to Automated Discovery in Geometry through Symbolic Computation, pages 257–271. Springer Vienna, Vienna, 2012.
[16] JÜRGEN RICHTER-GEBERT AND ULRICH KORTENKAMP. The Interactive Geometry Software Cinderella. Springer, 1999.
[17] SANA STOJANOVI´C, JULIEN NARBOUX, MARC BEZEM, AND PREDRAG JANIˇCI´C. A vernacular for coherent logic. In Stephen M.Watt, JamesH. Davenport, AlanP. Sexton, Petr Sojka, and Josef Urban, editors, Intelligent Computer Mathematics, volume 8543 of Lecture Notes in Computer Science, pages 388–403. Springer International Publishing, 2014.
[18] SANA STOJANOVI´C, VESNA PAVLOVI´C, AND PREDRAG JANIˇCI´C. A coherent logic based geometry theorem prover capable of producing formal and readable proofs. In Pascal Schreck, Julien Narboux, and Jürgen Richter-Gebert, editors, Automated Deduction in Geometry, volume 6877 of Lecture Notes in Computer Science, pages 201–220. Springer Berlin Heidelberg, 2011.
[19] ZHENG YE, SHANG-CHING CHOU, AND XIAO-SHA GAO. Visually dynamic presentation of proofs in plane geometry, part 2. J. Autom. Reason., 45:243–266, October 2010.
[20] ZHENG YE, SHANG-CHING CHOU, AND XIAO-SHAN GAO. An introduction to java geometry expert. In Thomas Sturm and Christoph Zengler, editors, Automated Deduction in Geometry, volume 6301 of Lecture Notes in Computer Science, pages 189–195. Springer Berlin Heidelberg, 2011.

S9 - Use of Mathematical Software in Research and Teaching

Educational graph creation tool based on the natural mathematical description

Tetsuo Fukui[1] [fukui@mukogawa-u.ac.jp]

[1] Mukogawa Women's University, Nishinomiya, Japan

In recent years, in the world including Japan, digital textbooks have been introduced into school education. Therefore, in mathematics education, it is important a tool enable students to create a graph easily on a digital device. However, the procedure to input the equation to define a graph by the existing current tool is still unnatural and troublesome for novice students. To address this shortcoming, we proposed an intelligent mathematical input interface, named MathTOUCH, in terms of predictive conversion from a colloquial style mathematical text using an AI in 2015 [1]. And in 2019, we have previously proposed a graph creation tool within the features [2]; 1st: it is implemented MathTOUCH, 2nd: it is enable us to create a graph based on the natural mathematical description, 3rd: to print a mathematical expression in the graph screen, 4th: to plot a point of ordered pair defined by a mathematical equation. However, this tool was based on a mathematics description only in Japanese not many national language. In addition, users had to switch the windows between the one editing the equation for a graph and the other of the graph main tool. In this study, we have improve the graph creation tool based on the natural mathematical description in English in addition to in Japanese and implemented MathTOUCH into the same window of this main tool as in an inline text. For example, the description to graph the equation $y = \sin^2 x$ is denoted by "graph of the equation $y = \sin^2 x$" and for the case to plot the peak point on the graph by "point $(\frac{\pi}{2}, 1)$". To investigate the effectiveness of this tool, we conducted a graph learning experiment by students in our University. The result showed that many students had high satisfaction for this tool.

Keywords
Graph, Equation, Mathematical input interface

References

[1] T. Fukui; S. Shirai, Predictive Algorithm from Linear String to Mathematical Formulae for Math Input Method. In *Booklet of Abstracts of the 21st Conference on Applications of Computer Algebra*, 17–22., Kalamata Greece, 2015.
[2] Y. Tominaga; N. Endo; T. Fukui, Proposal of graph creation tool based on the mathematical description (in Japanese). In *Kokyuroku*, vol. 2105, 69–78. RIMS, Kyoto Japan, 2019.

A teaching material for orthogonal transformation using rotation of cuboid

Naoki Hamaguchi[1] **,** ***Toshio Oshima***[2] **,** ***Setsuo Takato***[3] [hama@nagano-nct.ac.jp]

[1] General Education, National Institute of Technology, Nagano College, Japan
[2] Faculty of Science, Josai University, Japan
[3] Faculty of Science, Toho University, Japan

In mathematics classes at collegiate level, teachers often use materials for spatial figures such as graphs of two-variable functions or surfaces of revolution. Recently, these can be presented in various ways as follows.

1. Handouts to be distributed.
2. Slides to be presented on the screen.
3. Figures to be manipulated by students on tablets.
4. Physical models to be displayed or passed around.

These data of teaching materials are generated by KETCindy [1]. KETCindy also has functionality to easily make PDF-based presentation slides with flip animations, which are similar to so-called flip books. These slides are useful in class plans when combined with handouts, tablets, and physical models.

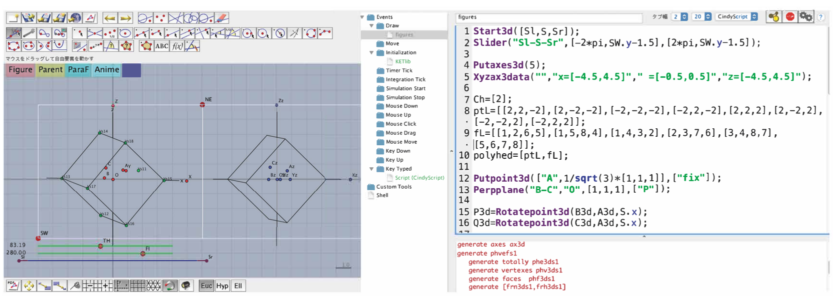


Figure 1: Cinderella screen and script

In this presentation, we will treat rotation of some types of cuboids around the axis through two opposite corners. This can be related to orthogonal transformation in three-dimensional Euclidean space. We will also show some examples of teaching materials presented in various ways about this theme.

The following part details the class plan. First, we use 3D physical models shown the left in Figure 2. We can spin the cube like the right in Figure 2.

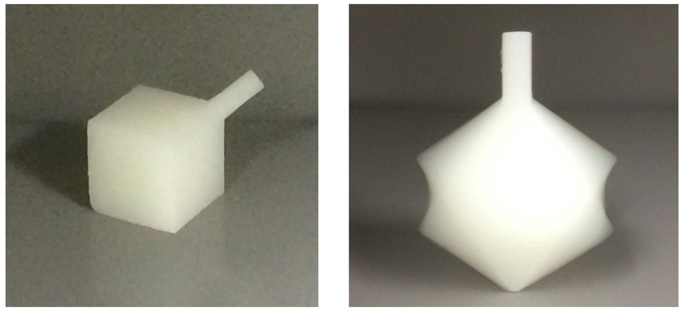


Figure 2

Secondly, we consider the axis of rotation. Let f be an orthogonal transformation. Assume that f maps $\mathrm{P}(1,\ 1,\ 1)$ to point P' on the x-axis.

We construct a right-handed orthonormal basis $\{\vec{u}_1,\ \vec{u}_2,\ \vec{u}_3\}$ such that $\vec{u}_1 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$, $\vec{u}_2$ is on the xy-plane, and z component of $\vec{u}_3$ is positive. Then, by $\vec{u}_1 \cdot \vec{u}_2 = 0$,

$$\vec{u}_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \quad \vec{u}_3 = \vec{u}_1 \times \vec{u}_2 = \frac{1}{\sqrt{6}}\begin{pmatrix} -1 \\ -1 \\ 2 \end{pmatrix}.$$

We explain $\vec{u}_1,\ \vec{u}_2$ and $\vec{u}_3$ by using figures on slides like those in Figure 3.

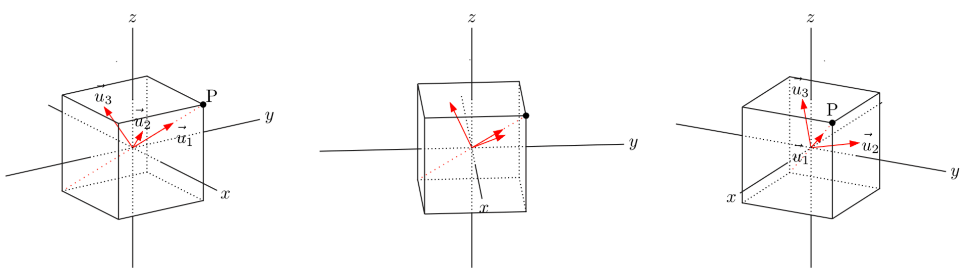


Figure 3

Put $T = (\vec{u}_1\ \ \vec{u}_2\ \ \vec{u}_3) = \begin{pmatrix} \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & 0 & \frac{2}{\sqrt{6}} \end{pmatrix}$, then $T\vec{e}_1 = \vec{u}_1,\ T\vec{e}_2 = \vec{u}_2,\ T\vec{e}_3 = \vec{u}_3$ hold for fundamental vectors $\vec{e}_1,\ \vec{e}_2,\ \vec{e}_3$. Since ${}^tT\vec{u}_1 = \vec{e}_1,\ {}^tT\vec{u}_2 = \vec{e}_2,\ {}^tT\vec{u}_3 = \vec{e}_3$, we can use the orthogonal matrix ${}^tT$ which represents f.

Using figures on slide like those in Figure 4, we explain that f maps segment QR to $\mathrm{Q}'\mathrm{R}'$. In this case, students can manipulate figures on tablets like those in Figure 5.

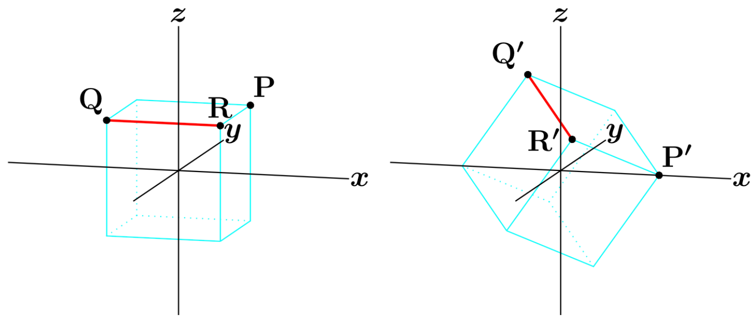


Figure 4

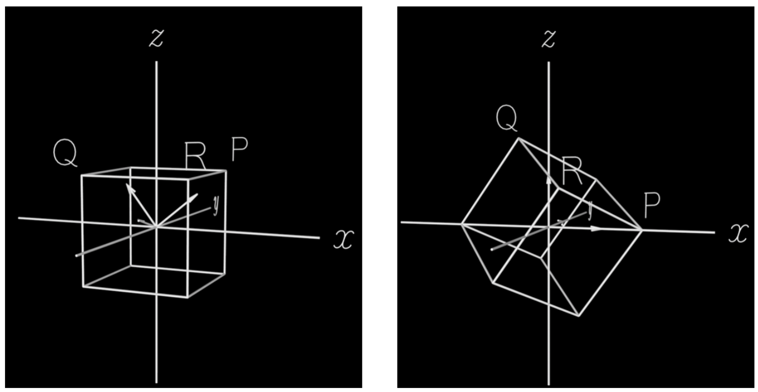


Figure 5

The segment QR is represented by

$$x = t,\ y = -1,\ z = 1\ (-1 \leqq t \leqq 1).$$

Multiplied by ${}^tT$, equations of Q′R′ is obtained as follows.

$$x = \frac{1}{\sqrt{3}}t,\ y = -\frac{1}{\sqrt{2}}(t+1),\ z = -\frac{1}{\sqrt{6}}(t-3)\ \ (-1 \leqq t \leqq 1).$$

Each vertex transformed by f, the cube is rotated around the x-axis. This is shown on slides like Figure 6.

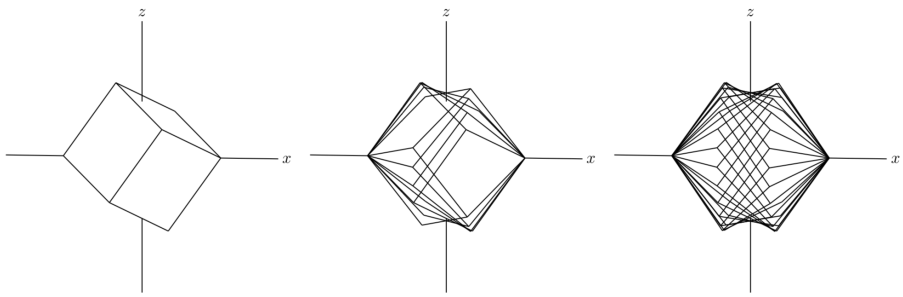


Figure 6

The upper slides in Figure 7 show intersection lines of face of this cube and plane $x = c$, and the lower include circles in rotating. The radius of circles are distance between the points on the segment and x-axis. Let C be intersection of zx-plane and the surface of revolution of the segment Q′R′. For the Point $(x,\ 0,\ z)$ on C,

$$z^2 = \left\{-\frac{1}{\sqrt{2}}(t+1)\right\}^2 + \left\{-\frac{1}{\sqrt{6}}(t-3)\right\}^2 = 2\cdot\frac{1}{3}t^2 + 2$$

Using $x = \dfrac{1}{\sqrt{3}}t$, we have $z^2 = 2x^2 + 2$, and hence, $x^2 - \dfrac{z^2}{2} = -1$.

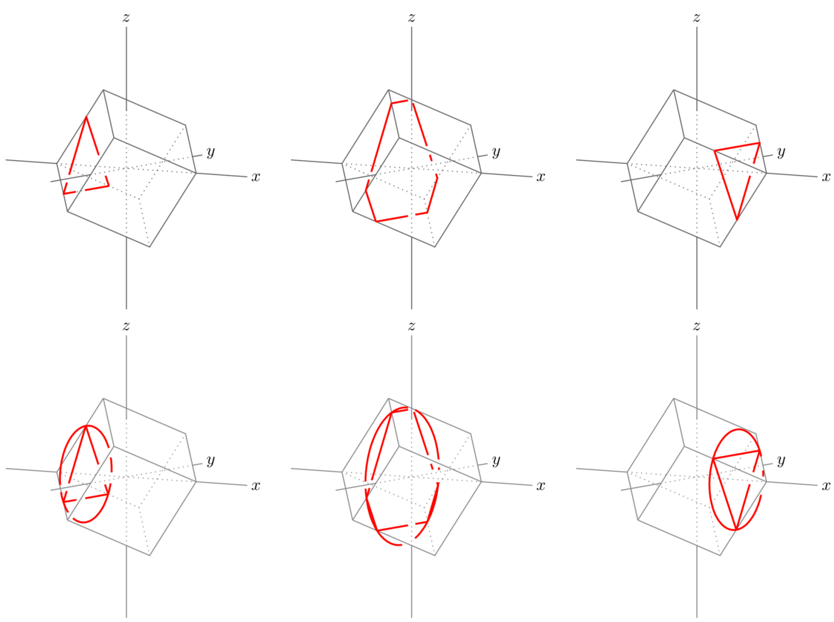


Figure 7

This rotation of cube can be shown as figures on tablets like those in Figure 8.

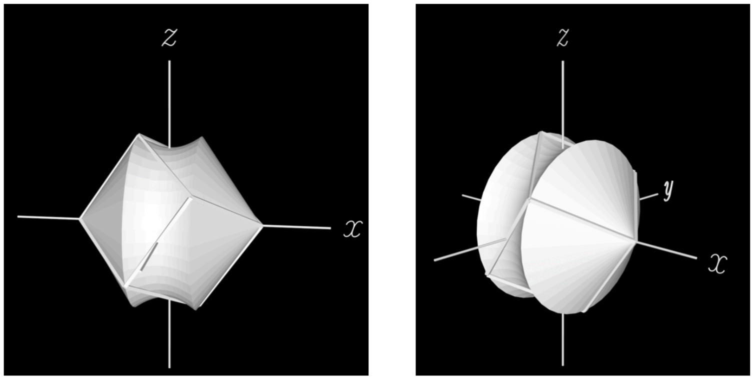


Figure 8

We can also make teaching materials of presentation slides for various types of cuboids as follows.

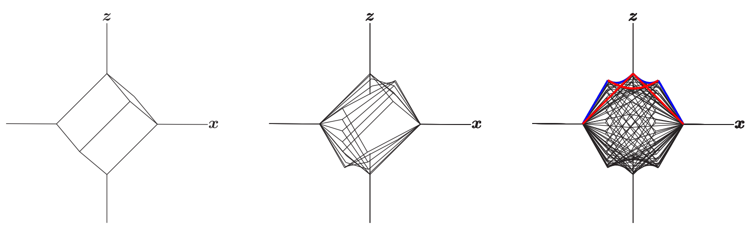


Figure 9: Case of $P(1,\ 1,\ \sqrt{2})$

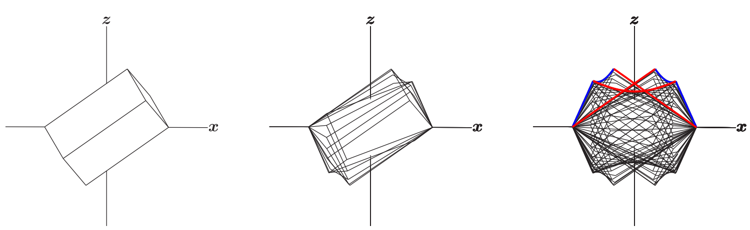


Figure 10: Case of $P(1,\ 1,\ 2)$

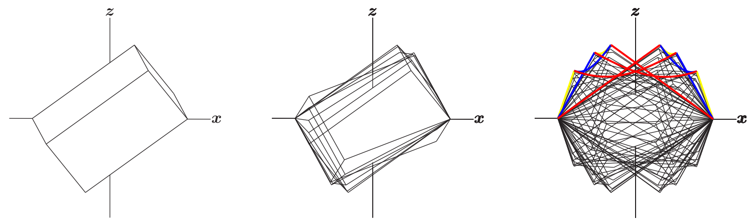


Figure 11: Case of P(2, 3, 5)

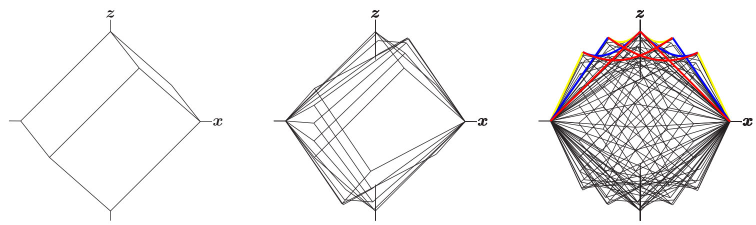


Figure 12: Case of P(3, 4, 5)

Keywords
KeTCindy, 3D models, spatial figures

References

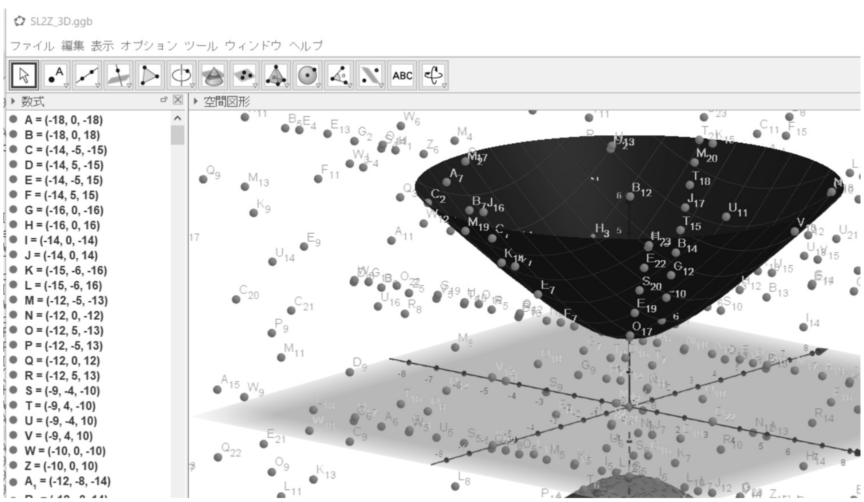
[1] N. HAMAGUCHI; S. TAKATO, Producing teaching materials for spatial figures with KeTCindy and the educational benefits of combining materials. In *Computational Science and Its Applications – ICCSA 2017, Part IV*, 262–272. Trieste, Italy, 2017.

Three-dimensional model of $SL(2,\mathbb{R})$ and visualization of $SL(2,\mathbb{Z})$ as a pattern on the cubic lattice

Yoichi Maeda[1] [maeda@tokai-u.jp]

[1] Department of Mathematics, School of Science, Kanagawa, Tokai University, Japan

It is known that real special linear group $SL(2,\mathbb{R})$ is embedded into the three-dimensional sphere [1]. We can see the three-dimensional sphere by the stereographic projection. Through this visualization, every matrix in $SL(2,\mathbb{R})$ is realized as a point in the three-dimensional Euclidean space $\mathbb{R}^3$. In this talk, we propose another three-dimensional model of $SL(2,\mathbb{R})$. With this model, we can visualize $SL(2,\mathbb{Z})$ as a pattern of points on cubic lattice in $\mathbb{R}^3$. For the purpose of this visualization, we combine two software: Python as CAS, and GeoGebra as DGS. In this model, the set of matrices with the fixed value of trace forms a quadratic surface (hyperboloid of two sheets, double cone, or hyperboloid of one sheet) depending on the value of trace. Hyperbolic paraboloid also comes out as the surface of the fixed value of element. With these familiar surfaces, we can analyze the pattern of $SL(2,\mathbb{Z})$.



Keywords
Three-dimensional model, $SL(2,\mathbb{R})$, $SL(2,\mathbb{Z})$, Quadratic surface

References

[1] Y. MAEDA, *Active Learning with Dynamic Geometry.* ICCSA 2017, Part IV, LNCS 10407, pp. 228-239, Springer (2017).

Fractals in the classroom with CAS and KeTCindy

Aleksandr Mylläri[1] **,** ***Tatiana Mylläri***[1] **,** ***Takeo Noda***[2]
Setsuo Takato[2] **,** ***Satoshi Yamashita***[3] [tmyllari@sgu.edu]

[1] St. George's University, Grenada, West Indies
[2] Toho University, Japan
[3] National Institute of Technology, Kisarazu College Department of Natural Science, Japan

We present our project of using Computer Algebra Systems (CAS) and Dynamic Geometry Systems (DGS) in teaching introductory course on Fractals. In our examples we use Wolfram *Mathematica* and KeTCindy.

Mathematica is very powerful CAS, it is easy to use, program codes are clear and compact, it has good graphic capabilities. KeTCindy is a plug-in to DGS Cinderella that generates high-quality TeX graphics. Moreover, KeTCindy makes it possible to import the data calculated or simulated by using other systems (like Maxima, Scilab, and R) and combine them with the graphical data, so that extremely wide range of mathematical objects can be presented.

Classic fractals (Sierpinski gasket, Sierpinski carpet, Mandelbrot set, and others) are used for examples and demonstrations. Different approaches and paradigms are used to construct fractal sets: Game of chaos, Multiple Reduction Copy Machines, and others. We give examples of codes and workbooks making a special stress on using KeTCindy.

Depending on the situation and final goal, both *Mathematica* and KeTCindy can be used in the classroom, or preference could be given to one of the systems. As was mentioned earlier, *Mathematica* is easy to use, but it is expensive and, in a way, it is too easy to use, it doesn't expand horizon for the students. From the other side, KeTCindy is not as easy to start using, but it is free and encourages students (and faculty) to study/use R, Maxima, etc. In addition, some dynamical visualizations seem easier to do with KeTCindy than in *Mathematica*.

Keywords
Fractals, Dynamic Geometry Systems

Effective Use of KeTCindy in an Experimental Study to Develop Methods of Teaching Mathematics

***Koji Nishiura*[1], *Masaki Suzuki*[2], *Setsuo Takato*[3], *Kunihiti Usui*[4]** [nishiura@fukushima-nct.ac.jp]

[1] General Education, National Institute of Technology, Fukushima College, Japan
[2] General Education, National Institute of Technology, Numazu College, Japan
[3] Faculty of Sciences, Toho University, Japan
[4] Control Engineering, National Institute of Technology, Kisarazu College, Japan

In this study, we determine the aspects of mathematics that students of upper secondary and higher education find difficult to understand. Our research aims to create an effective method of teaching mathematics and to develop enhanced materials for teaching the topics that students find problematic. For these purposes, we conduct an experimental study using our previously developed Cognitive Detection Clicker, which facilitates recording of students' responses along with response times [1].

To create mathematics teaching materials, teachers often generate graphics. Although TEX is a popular tool to generate high-quality mathematical expressions or formulas in printed teaching materials, generating high-quality graphics in TEX documents is not easy. To overcome this difficulty, KETCindy mathematical software is developed, which is a plug-in program for Cinderella dynamic geometry software [2]. It converts the procedure of drawing graphical objects on the Cinderella screen into TEX readable code, thus generating corresponding high-quality mathematical artwork in the final PDF output. Furthermore, KETCindy is implemented with a function of calling other computing tools such as R and Maxima and many other additional functions [3].

We use KETCindy in our experimental process, starting from creation of teaching materials to analysis of the results. In this talk, we will present those functions of KETCindy used in our experimental study.

Keywords
KeTCindy, experimental study, methods of teaching mathematics

References

[1] K. NISHIURA, S. OUCHI, K. USUI, Analysis of the Use of Teaching Materials Generated by KeTCindy as an Aid to the Understanding of Mathematics, *Lecture Notes in Computer Science* **10407**(4), 216–227 (2017).
[2] M. KANEKO, S. YAMASHITA, K. KITAHARA, Y. MAEDA, Y. NAKAMURA, U. KORTENKAMP, S. TAKATO, KETCindy–Collaboration of Cinderella and KETpic, *The International Journal for Technology in Mathematics Education*, **22**(4), 179-185 (2015).

[3] M. Kaneko, S. Yamashita, H. Makishita, K. Nishiura, S. Takato, Collaborative use of KETCindy with other small tools, *The Electronic Journal of Mathematics and Technology*, **11**(2), 100-111(2017).

Visualizing ODEs with KeTCindy

Takeo Noda[1] [noda@c.sci.toho-u.ac.jp]

[1] Faculty of Science, Toho University, Japan

In ordinary differential equations courses, not only techniques of solving equations but also theoretical and qualitative aspects should be treated. To teach those aspects efficiently, visual teaching materials are always desirable. For example, visualizing a differential equation as a slope field will help learners to understand the existence of local solutions or the difference of local and global solutions. Also, bifurcation pheonomena will be understood clearly if they are expressed in animation forms.

KeTCindy is a powerful tool for generating such mathematical figures. It uses Cinderella as a graphical user interface and creates TeX codes for the graphics. The outputs can be implemented not only in printed matters, but also in slides for screen presentation. Furthermore, KeTCindyJS, which is an extended version of CindyJS, can make those figures into interactive content which can be viewed and manipulated on web browsers.

In this talk, we will show visual teaching materials which are made by using KeTCindy and used in a course of ordinary differential equations.

Keywords
ordinary differential equations, KeTCindy, CindyJS

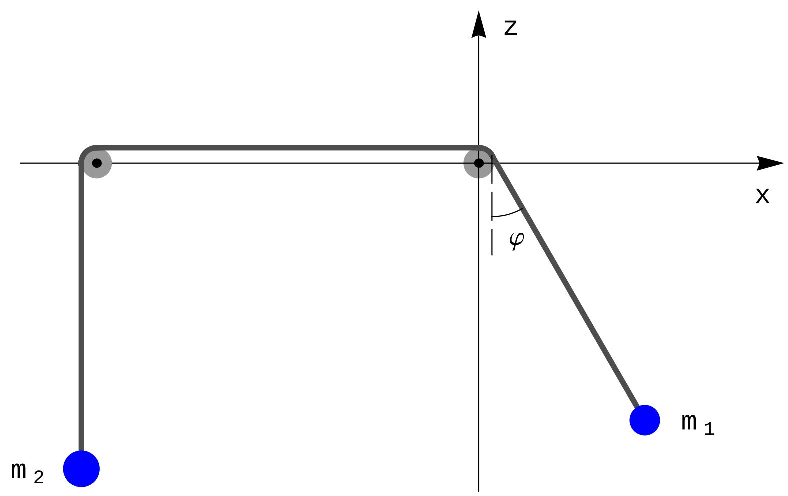
Animation of some mechanical systems with Mathematica

Alexander Prokopenya[1]***, Setsuo Takato***[2] [alexander_prokopenya@sggw.pl]

[1] Department of Applied Informatics, Warsaw University of Life Sciences, Warsaw, Poland
[2] Faculty of Science, Toho University, Funabashi, Japan

It is well known that the computer algebra system Mathematica (see [1]) is a powerful tool for doing both numerical and symbolic computation. Its built-in functions $DSolve$ and $NDSolve$ enable to solve easily differential equations describing motion of different mechanical systems and to visualize the results. Besides, using these solutions, one can animate the system and demonstrate its motion what is very interesting and useful for education.

As an example, let us consider a generalized version of the simple Atwood machine (see [2]) when two bodies of masses m_1, m_2 ($m_2 \geq m_1$) are attached to opposite ends of a massless inextensible thread wound round two massless frictionless pulleys of negligibly small radius.



Two separated pulleys are used here to avoid collisions of the bodies. Body m_2 is constrained to move only along a vertical while body m_1 swings in a vertical plane. Such a system has two degrees of freedom and its motion is described by the following differential equations (see [3])

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

Here r is a length of the thread between pulley and body m_1, the angle φ describes deviation of the thread from the vertical, g is a gravitational constant, and parameter $\mu = m_2/m_1$.

Note that equations (1) are nonlinear and their general solution cannot be obtained in symbolic form. Numerical analysis has shown (see [3]) that even small oscillation of the body

m_1 can modify the system motion significantly and some unexpected kind of motion such as quasi-periodic one can arise.

In the present talk we use a numerical solution of equations (1) obtained for some realistic values of the system parameters and discuss the problem of animation of the generalized Atwood machine with Wolfram Mathematica. Our aim is to describe step by step a process of constructing a graphical object used for animation and to demonstrate a final result.

The animations in PDF or HTML format can be produced by KeTCindy which the second author has developed.

Keywords
Atwood's machine, Simulation, Quasi-periodic motion, Mathematica

References

[1] S. Wolfram, *An elementary introduction to the Wolfram Language, 2nd ed.*. Champaign, IL, USA, Wolfram Media, 2017.
[2] G. Atwood, *A Treatisa on the Rectilinear Motion and Rotation of Bodies.* Cambridge University Press, 1784.
[3] A.N. Prokopenya, Motion of a swinging Atwood's machine: simulation and analysis with Mathematica. *Mathematics in Computer Science* **11**, 417–425 (2017).

Symbolic and numerical study of Fourier series and PDEs using Maxima

Emmanuel Roque[1] **, _José A. Vallejo_**[1] [emmanuelroquej@protonmail.ch]

[1] Faculty of Sciences, Autonomous University of San Luis Potosí, México

in both bounded and unbounded domains, and various types of initial conditions. In the bounded domain case, the basic idea is to apply the separation of variables method which leads to a well-defined algorithm for developing the solution in a Fourier series. Therefore, this problem is tractable with a Computer Algebra System (CAS). In this work we introduce a Maxima package (called pdefourier) to solve it. The package is able to compute the Fourier series of a function both numerically and symbolically, admitting piecewise-defined functions as arguments. It contains solvers for the onedimensional heat and wave equations on a domain [a; b] with general boundary conditions of the form

$$\alpha_1 u(0,t) + \beta_1 u_x(0,t) = f_1(t)$$
$$\alpha_2 u(L,t) + \beta_2 u_x(L,t) = f_2(t)$$

Also, the package can solve the two-dimensional Laplace equation for a variety of domains (rectangles, disks, annuli, wedges) and boundary conditions (Dirichlet, Neumann and mixed).

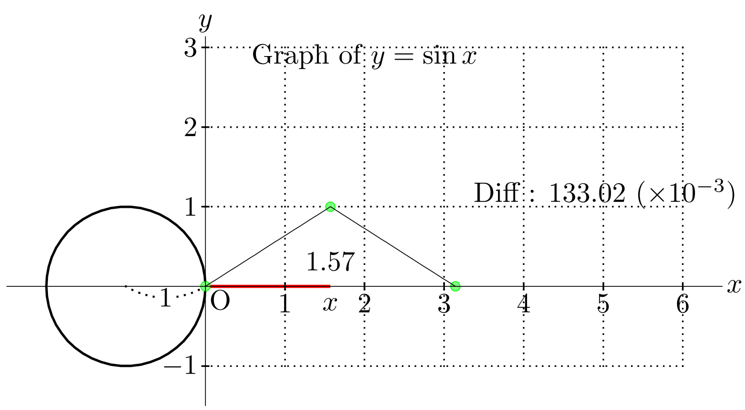
Keywords: Fourier Analysis, PDEs, Mathematical Software.

Development and Applications of KeTCindyJS

Setsuo Takato[1] [takato@phar.toho-u.ac.jp]

[1] Faculty of Science, Toho University, Funabashi, Japan

KeTCindy[3] is a collaboration of KeTpic we developed to produce LaTeX figures and Cinderella[1], a DGS. KeTCindy works as a kind of preprocessor of graphical code system such as pict2e or tikz, and mathematics teachers can produce their printed materials with figures easily and interactively. Meanwhile CindyJS has been developed by the group of Technical University of Munich. They has produced various fine geometric figures [2]. However, teachers will want produce material of not only geometry. So we have developed KeTCindyJS which adds functions of KeTCindy to CindyJS. Using KeTCindyJS, teachers can produce various interactive materials easily. The following is an example of such materials.



The above file is accesible at
`https://s-takato.github.io/ketcindysample/aca2019/`

Anyone can dowload KeTCindy package freely from CTAN:
`https://ctan.org/pkg/ketcindy`.

Keywords
Cinderella, CindyJS, KeTCindy

References

[1] Cinderella, https://www.cinderella.de/tiki-index.php
[2] CindyJS, https://cindyjs.org
[3] S. Takato; A. McAndrew; J.A. Vallejo; M. Kaneko,Collaborative use of KeTCindy and free Computer Algebra Systems. *Mathematics in Computer Science* **11**, 503–514 (2017).

Extension of KeTCindyJS to generate interactive HTML slides

***Koji Nishiura*[1], *Setsuo Takato*[2], <u>*Tomoya Tokairin*</u>[3],** [tokai@hakodate-ct.ac.jp]

[1] National Institute of Technology, Fukushima College, Japan
[2] Toho University, Japan
[3] National Institute of Technology, Hakodate College, Japan

In the session we are going to present an extension of KeTCindyJS [1] to generate interactive HTML slides. We are also going to show demonstrations. KeTCindyJS is an extension of CindyJS [2], and is able to generate HTML files by several functions of KeTCindy on Cinderella [3]. So far, KeTCindyJS is not able to generate HTML slides by PDF slide generating functions such as Settitle(). Thus, we have been extending KeTCindyJS for HTML slide generation. This extension makes it easy for teachers to generate HTML slides by intermediate code which is compatible with KeTCindy. Furthermore, this extension helps students learn their subjects, because they can view the generated slides as teaching materials with mobile devices anytime, anywhere.

Keywords
teaching materials, Cinderella, Tex, JavaScript

References

[1] `http://ketpic.com/?lang=english`
[2] `https://cindyjs.org`
[3] `https://cinderella.de`

Calculation and visualization of Fourier series with KeTCindy and KeTCindyJS

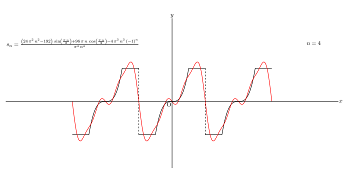
***Setsuo Takato*[1], *José A. Vallejo*[2], <u>*Satoshi Yamashita*</u>[3]** `[yamasita@kisarazu.ac.jp]`

[1] Faculty of Science, Toho University, Funabashi, Japan
[2] Faculty of Science, State University of San Luis Potosí, México
[3] Division of Natural Science, National Institute of Technology, Kisarazu College, Japan

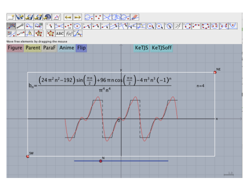
When teaching a course on Fourier analysis or its applications, as important as to learn how to compute Fourier coefficients, is to be able to understand the geometric meaning of finite Fourier series, and get a feeling about their convergence to given periodic functions. In this contribution, we introduce a software-based tool to create visually appealing graphics and animations of Fourier series based on the use of KeTCindy and KeTCindyJS. KeTCindy is a plug-in for Cinderella2, originally developed as a kind of pre-processor of TeX graphical code systems such as tpic, pict2e and TikZ. Cinderella2 works as a graphical user interface of KeTCindy in such a way that one can create figures for TeX documents interactively and easily. Recently it has enhanced in two ways: now it is able to call the CAS Maxima and to produce HTML files with the help of CindyJS. The combination of CindyJS and KeTCindy has originated the set of macros 'KeTCindyJS'. We show examples of its use in Fourier analysis, explaining how they are obtained using the following elements:

1. A Maxima package called 'pdefourier.mac for the numeric and symbolic computation of Fourier series'
2. A function 'Periodfun' to translate function definitions to Maxima syntax.
3. A function 'Ketcindyjsdata' to embed the results from Maxima into the HTML file generated by KeTCindyJS.

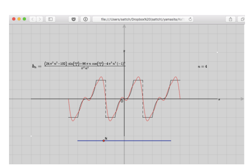
The following samples are downloadable from https://sattch.github.io.



PDF



CindyScreen



KeTCindyJS

1 The Maxima package ‘pdefourier.mac’

The Maxima package ‘pdefourier.mac’, enables us to compute the Fourier coefficients of any periodic function, even if it is piecewise-defined. For example, let $f(x)$ be a periodic function with period 4 defined by the equation

$$f(x) = \begin{cases} -2 & (-2 \leqq x < -1) \\ 2x^3 & (-1 \leqq x < 1) \\ 2 & (1 \leqq x < 2)\ . \end{cases}$$

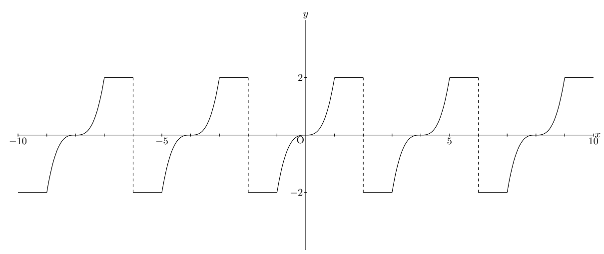


Figure 1

We first load the package and then compute the Fourier coefficients of $f(x)$ in the following KeTCindy script:

```
1  f0="if (-2<=x and x<-1) then -2 elseif (-1<=x and x<1)
        then 2*x^3 elseif (1<=x and x<2) then 2";
2  period=4;
3  cmdL=Concat(Mxbatch("pdefourier.mac"),[
4    "f0(x):="+f0,[],
5    "c:fouriercoeff",["f0(x)","x",period],
6    "c:c[1]",[],
7    "c[1]::c[2]::c[3]",[]
8  ]);
9  CalcbyM("ans",cmdL,[make,"Err=n"]);
```

Let us explain the syntax: In the first line we define $f(x)$ as `f0`. The call to `CalcbyM` in line 9 includes the execution of the command `cmdL`, which runs in batch mode the commands from lines 3 to 8, storing the output in `ans`. Notice that ‘pdefourier.mac’ is loaded by `Mxbatch` in the 3rd line. Finally, the output `ans` contains the Fourier coefficients $[a_0, a_n, b_n]$:

```
[0,0,((24*%pi^2*n^2-192)*sin((%pi*n)/2)+96*%pi*n*cos((%pi*n)/2)
       -4*%pi^3*n^3*(-1)^n)/(%pi^4*n^4)]
```

Notice that $a_0 = 0 = a_n$, as it should be for an odd periodic function.

2 The function 'Periodfun'

In the previous example we followed the syntax required by the package 'pdefourier.mac', which is oriented towards the natural language. However, for internal efficiency it is better to work in a more direct manner, just giving the values on the sub-intervals of definitions. Thus, instead of writing

```
f0="if (-2<=x and x<-1) then -2 elseif (-1<=x and x<1)
    then 2*x^3 elseif (1<=x and x<2) then 2";
```

we could use the function 'Periodfun' in KeTCindy, as follows:

```
1  defL=[
2   "-2",[-2,-1],1,
3   "2*x^3",[-1,1],50,
4   "2",[1,2],1
5  ];
6  tmp=Periodfun("a",defL,"x",["Con=da"]);
7  f0=tmp_1;
8  period=tmp_2;
```

In lines 1–5, `defL` is used to define $f(x)$. In line 6, the calling to `Periodfun` creates the list `tmp` and draw the graph of the function $f(x)$ in the dynamic geometry screen of Cinderella2 as is shown in Figure 1. The elements of `tmp` are:

```
[if (-2<=x and x<-1) then -2 elseif (-1<=x and x<1) then 2*x^3
 elseif (1<=x and x<2) then 2,4]
```

The list `tmp` has two arguments: one is the definition of the function $f(x)$ in Maxima and the other the period 4 of the function $f(x)$.

3 The function 'Ketcindyjsdata'

Cinderella2 can produce HTML files using CindyJS, but CindyJS cannot process data generated by KeTCindy, to be included in the HTML. To overcome this drawback, we developed the macro 'KeTCindyJS'. However, in its first incarnation KeTCindyJS was unable to process data generated from Maxima. Consequently, we added the a function 'Ketcindyjsdata' to KeTCindy, which now includes communication capabilities between KeTCindyJS and Maxima. As an example, consider the following code:

```
 9  CalcbyM("ans",cmdL,[make,"Err=n"]);
10  Ketcindyjsdata(["ans",ans]); //no ketjs off
```

In line 10, `Ketcindyjsdata` inputs the list `ans` generated by Maxima in the HTML file 'fourierjson.html' as follows:

```
ans=[0,0,"((24*%pi^2*n^2-192)*sin((%pi*n)/2)+96*%pi*n*cos((%pi*n)/2)
     -4*%pi^3*n^3*(-1)^n)/(%pi^4*n^4)"];
```

The resulting HTML file 'fourierjson.html' with the embedded javascript is shown in Figure 2.

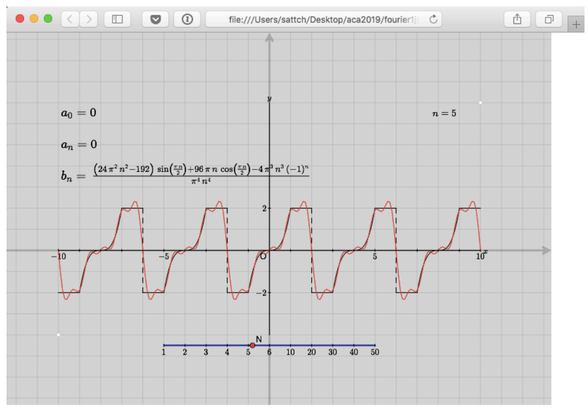


Figure 2

KeTCindyJS can generate HTML files that can be viewed even offline, so `Ketcindyjsdata` is not needed on the part of the user.

4 Conclusions

There is available a powerful environment combining a free CAS such as Maxima, the DGS Cinderella2, and the macros set KeTCindy (with KeTCindyJS), allowing to study Fourier developments both from the purely analytic point of view and the geometric one. We think that the possibility of creating animations in a straightforward manner, that can be included in HTML web pages, and printed from pdf files containing high-quality graphics, can be very useful for university teachers and researchers.

Keywords
KeTCindy, KeTCindyJS, Cinderella2, CindyJS, Maxima, Fourier series

Poster Session

Manipulating symbolic expressions on a computer

Koissi Adjorlolo[1,2] [adjorlolo.k@husky.neu.edu]

[1] Khoury College of Computer Science, Northeastern University, Boston, Massachusetts
[2] Mathematics Department, College of Science, Northeastern University, Boston, Massachusetts

Advisors: David Sprague[1], Anthony Iarrobino[2]

I present preliminary work on Shoreline, an application that allows high school math students to manipulate symbolic expressions on a computer as an alternative to paper. A computer-based method for working with symbolic expressions has the ability to control how a user solves certain problems, which could offer the user insight into the problem that they might have missed while solving the same kind of problem on paper. Prior attempts at achieving this, such as the iOS application Algebra Touch [1][2] have been limited in scope, but their strengths and weaknesses were compared to Shoreline's design during its development.

Shoreline presents its user with a symbolic expression and a list of identities that can be applied to that expression. The user can match an identity to the expression by selecting different parts of the expression. Identities that match the selection can be clicked by the user to transform the selected parts of the expression into another form. This method of interaction stresses that the user learns when an identity can be applied and how exactly to apply the identity. This can't be stressed to a student solving the same problems on paper without significantly slowing down the problem-solving process.

Shoreline currently works with basic algebraic expressions. Future work will explore the extent to which this system can represent different kinds of symbolic manipulations within mathematics.

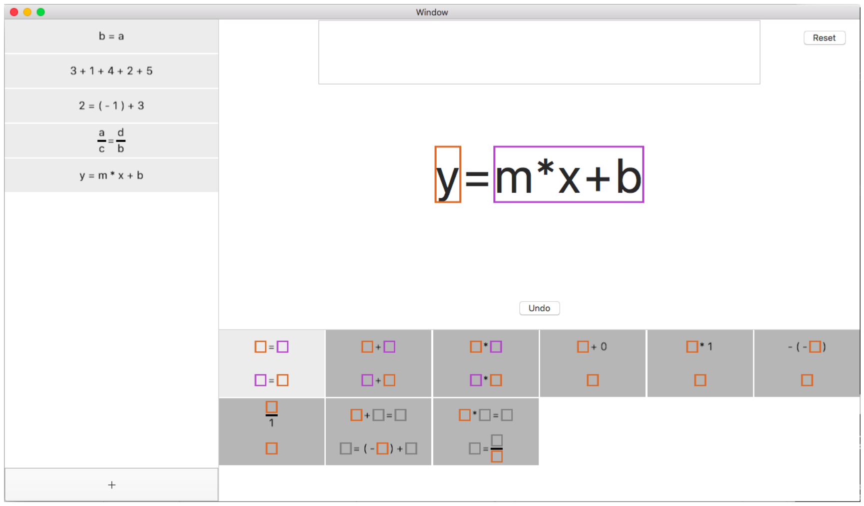


Figure 1: Shoreline with an example selection of the main expression

Keywords
Education, Symbol-manipulation, Mathematics, Alternative to paper, Computer Science

References

[1] S. BERRY, *Algebra Touch*. Regular Berry Software LLC. Version 2.2.11.

[2] E. OTTMAR, D. LANDY, R. GOLDSTONE, Title. *Proceedings of the Annual Meeting of the Cognitive Science Society* **34**(34), 2156–2161 (2012).

Software in the Wolfram Language for Real Algebraic Curves

Barry H. Dayton[1] [barry@barryhdayton.us]

[1] Emeritus, Department of Mathematics, Northeastern Illinois University,Chicago, Illinois

Mathematica functions are given to create, transform and represent real curves given by systems of polynomials with, possibly, numeric coefficients using mostly numerical algorithms. These are divided into three parts, plane curves given by a single bivariate polynomial, curves in $\mathbb{R}^3$ defined by 2 polynomials in 3 variables and curves in $\mathbb{R}^n, n \geq 3$ defined by a system of $n-1$ or more equations. Although the curves are given in affine form ultimately they are considered as projective curves. The transformations are projective linear transformations, sometimes called linear fractional transformations or fractional linear transformations.

The first case of plane curves is given in my book [1,2] and/or freely available Wolfram notebooks [1,3]. In addition to well known curves, constructions are given for two classes of real curves, one given by Gauss in his 1799 proof of the Fundamental Theorem of Algebra the other motivated by Newton's work on cubic curves. Curves are analyzed by finding critical and infinite points and tracing paths between them. Because the projective plane is compact this is a finite process. Representations include plotting on the Möbius band. All code is available at [3].

The other two cases in this poster are from a second volume currently in the writing phase. A summary of what is available now is given in [3] along with the code. The case of 2 polynomials in $\mathbb{R}^3$ is similar to the plane case thanks to the availability of the cross product. The last case is handled by projecting to the plane, analyzing as in the first case, and lifting, all using lots of numerical linear algebra.

The one general concept running through all cases is the *Fundamental Theorem* which states that each algebraic real curve can be represented by a graph with vertices certain projective points on the curve and edges non-singular paths between vertices. These graphs have the property that each vertex is even.

Keywords
Algebraic Curves, Numerical Algebraic Geometry, Wolfram Language

References

[1] Barry H Dayton, *A Numerical Approach to Real Algebraic Curves*. Wolfram Media, 2018. Available at `Wolfr.am/Dayton`.
[2] Barry H Dayton, A Wolram Language Approach to Numerical Algebraic Plane Curves *The Mathematica Journal* **20**(August 29, 2018), Free PDF from `mathematica-journal.com`.
[3] Barry H Dayton, website `https://barryhdayton.space`.

Automatic Generation of Inverse Dynamics for Industrial Robots with Flexible Joints Using a Computer Algebra

***Thanh-Trung Do*[1], *Zhaoheng Liu*[1], *Viet-Hung Vu*[1]** `[thanh-trung.do.1@ens.etsmtl.ca]`

[1] Department of Mechanical Engineering, École de technologie supérieure,
Montreal, Canada

The use of industrial robots in modern manufacturing technologies receives more attention from researchers and engineers in recent years. However, the robotic machining systems have generally lower rigidity than the traditional CNC machines due to the presence of compliant transmission elements that cause poor performance. To overcome this drawback and reduce vibration of the robot's end-effectors, model-based controllers which incorporate dynamic system equations of the robot should be used. Generally, the inverse dynamics problem of flexible-joint robots is much more complicated than that of rigid-joint robots because it requires computing second-time derivatives of actuated forces/moments. In this work, we present a new algorithm based on the recursive Newton-Euler algorithm and Maple to automatically generate inverse dynamics for any industrial flexible-joint robot in symbolic form which can be used for real-time control and numerical simulations. The only input to our algorithm is a numeric/symbolic matrix basically containing the Denavit-Hartenberg as well as physical parameters of robots. The efficiency of the proposed algorithm is compared to existing approaches.

Keywords
Flexible-joint robots, Inverse dynamics, Model-based control, Symbolic computation.

References

[1] A. De Luca; W. Book, *Robots with flexible elements.* In *Springer Handbook of Robotics.* Editors: B. Siciliano and O. Khatib, 2016.
[2] G. Buondonno; A. De Luca, A recursive Newton-Euler algorithm for robots with elastic joints and its application to control. In *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 2015.
[3] G. Swiatek; Z. Liu; B. Hazel, *Dynamic simulation and configuration dependant modal identification of a portable flexible-link and flexible-joint robot.* In *28th Seminar on Machinery Vibration*, 2010.

HNN-extension of free Rota-Baxter Lie algebras

Chia Zargeh[1] [chia.zargeh@ufba.br]

[1] Departamento de Matemática, UFBA, Salvador, BA, Brazil

On the basis of Groebner-Shirshov bases for free Rota-Baxter Lie algebras [2], we introduce a specific technique for spreading the notion of HNN-extension of groups to the case of free Rota-Baxter Lie algebras in order to obtain an embedding theorem. We recall that HNN-extension of groups states that if A_1 and A_2 are isomorphic subgroups of a group G, then it is possible to find a group H containing G such that A_1 and A_2 are conjugate to each other in H and G is embeddable in H (see [1]). The concept of HNN-extension of free Rota-Baxter Lie algebras is constructed through employing a differential K-algebra of weight λ, that is, an associative K-algebra R together with a linear operator $d : R \to R$ such that

$$d(xy) = d(x)y + xd(y) + \lambda d(x)d(y), \; \forall x, y \in R,$$

and

$$d(1) = 0,$$

where K is unitary commutative ring and $\lambda \in K$. This operator is called a derivation of weight λ or a λ-derivation.

Keywords
HNN-extension, Rota-Baxter algebra, Groebner-Shirshov basis

References
[1] G. Higman; B.H. Neumann; H. Neumann, Embedding theorems for groups. *J. London. Math. Soc,* **24** (MR:11:322d), 247–257, (1949).
[2] J. Qiu, Y. Chen, Groebner–Shirshov bases for Lie Ω-algebras and free Rota-Baxter Lie algebras, *Journal of Algebra and Its Applications*, **16**(2), 175–190 (2017).

Partenaires | Sponsors

Le comité organisateur de ACA 2019 est reconnaissant envers tous ses précieux partenaires qui ont contribué au succès de l'événement.

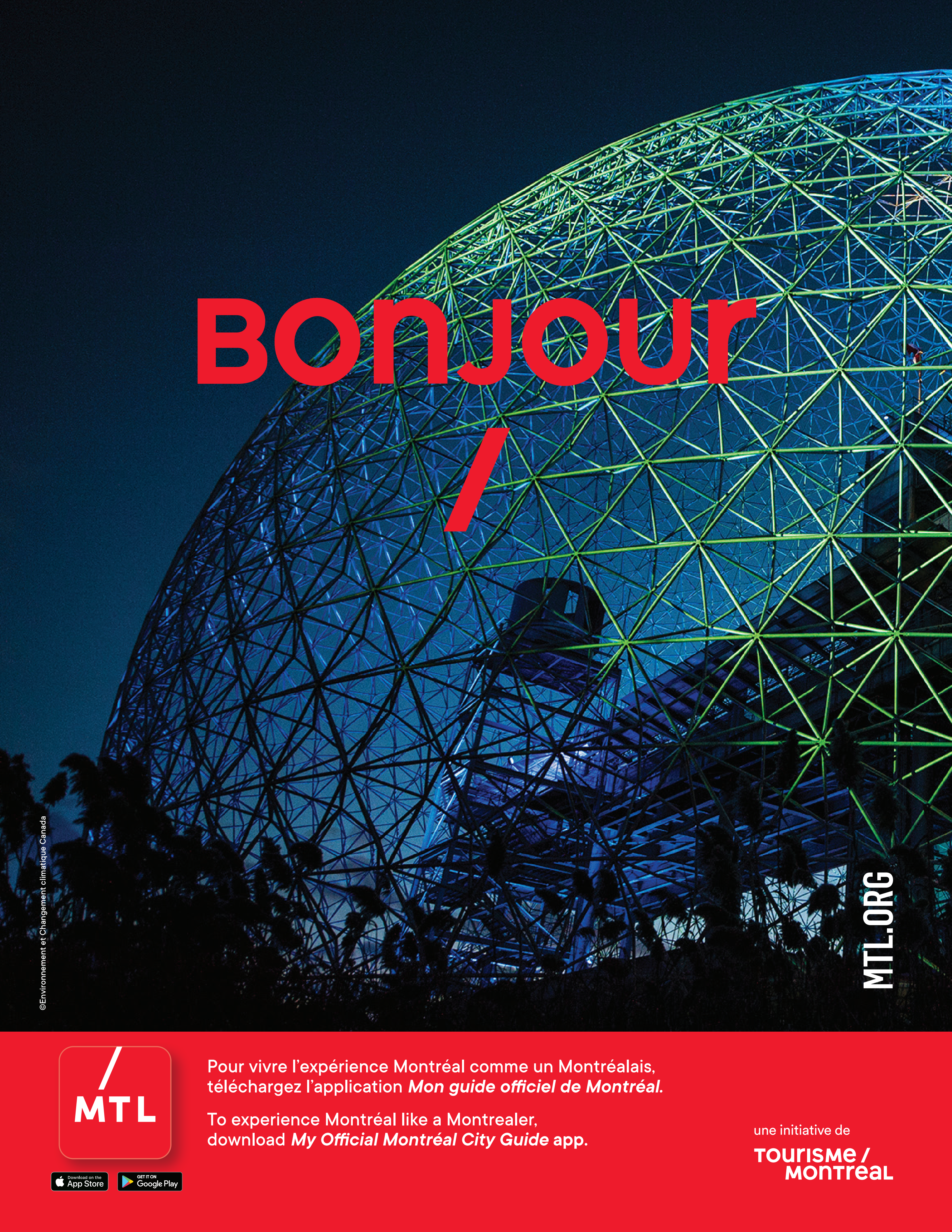
The ACA 2019 organizing conference is deeply grateful to all its sponsors. Their contributions have been fundamental in making this event a success.

Platine | Platinum

Or | Gold

Argent | Silver

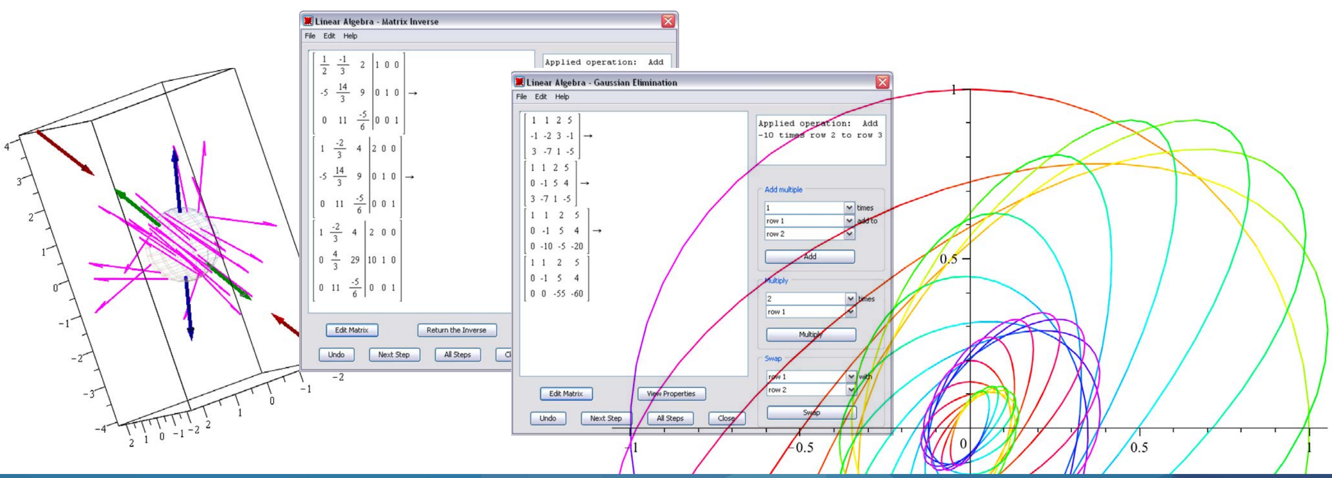
Bronze | Bronze


BONJOUR
/
MTL.ORG
©Environnement et Changement climatique Canada
/
MTL
Download on the App Store
GET IT ON Google Play
Pour vivre l'expérience Montréal comme un Montréalais,
téléchargez l'application *Mon guide officiel de Montréal.*
To experience Montréal like a Montrealer,
download *My Official Montréal City Guide* app.
une initiative de
TOURISME / MONTRÉAL

Maple™

Maple lets you solve more problems, more easily

- Over 5000 functions covering virtually every area of mathematics, including algebra, differential equations, statistics, calculus, linear algebra, graph theory, differential geometry, number theory, and much more
- Symbolic, numeric, and hybrid computation algorithms
- World-leading algorithms for solving problems that are beyond the reach of any other software system
- Sophisticated 2-D and 3-D plotting and animations
- Efficient algorithms and tools for high performance computing and large-scale problem solving
- Sophisticated programming language designed for mathematics
- Rich authoring environment for creating technical documents and applications



For more information on the latest version of Maple, please visit

www.maplesoft.com/Maple2019

Maplesoft

www.maplesoft.com | info@maplesoft.com • Tel: +49 241 980919 30

© Maplesoft, a division of Waterloo Maple Inc., 2019. Maplesoft, Maple, and MapleSim are trademarks of Waterloo Maple Inc. All other trademarks are the property of their respective owners.