21st Conference on Applications of Computer Algebra

ACA 2015

July 20 - 23, 2015
Elite City Resort
Kalamata, Greece

http://www.singacom.uva.es/ACA2015/

General Chair:

Ilias Kotsireas

Program Chair:

Edgar Martínez-Moro

Advisory Committee:

Eugenio Roanes-Lozano
Stanly Steinberg
Michael Wester

Publicity:

Zafeirakis Zafeirakopoulos

Contents

Sponsors

Maplesoft™

Mathematics • Modeling • Simulation

A Cybernet Group Company

Texas Instruments

MR & Associates Ltd

Leaders in Scientific Software

Wilfrid Laurier University

Sibi Domvm Sapientia Aedificavit

Universidad de Valladolid

Foreword

Dear Participants,

it is our great pleasure to welcome you to Kalamata for the 21st edition of the Applications of Computer Algebra conference, ACA 2015. We want to acknowledge the hard work of all the Session Organizers, that is a crucial element of the success of every conference in the ACA conference series. Two other important aspects of ACA 2015 are the Twitter account `@2015_ACA` and the refereed Springe PROMS proceedings (`http://www.springer.com/series/10533`). We hope that both will contribute to the success of the conference.

According to the advice of Stanly Steinberg, founder of the ACA conference series and Michael Wester, co(n)-founder of the ACA conference series, as cited in

`http://math.unm.edu/ aca/ACA/Organizing/Traditions`:

”*The conference chairs are the autocrats. The ACA working group can advise (as well as anyone who wishes to contact any member of the working group), but whomever is the chair (or chairs) have final authority over how the conference they are organizing is run. This is only fair, because organizing is a huge amount of work (but the rewards are great), so the chairs should not be burdened by dilution of authority. (Anyone who has chairs a conference is a bit crazy, either before or certainly afterwards!) The hard work of the chairs are appreciated by all who participate in the conference and any problems should be diplomatically discussed with them.*”

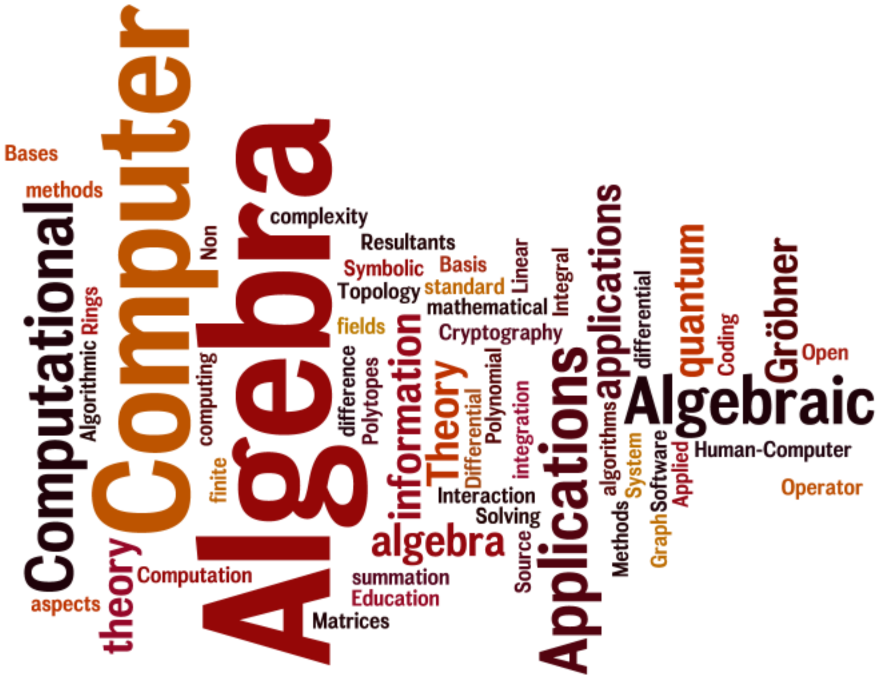
Therefore we would like to express a resounding THANK YOU to a very energetic and enthusiastic group of people, namely the ACA WG (Working Group) for their invaluable help and unwavering support to us, as ACA 2015 Organizers. Their contributions to the organization of ACA conference over the years are indeed priceless.

We are also very grateful to our sponsors and last but not least we would like to thank a long list of student volunteers, that make ACA 2015 possible, through their hard work and dedication.

We sincerely hope that you will thoroughly enjoy your stay in Kalamata for ACA 2015 and your stay in Greece in general.

Edgar Martínez-Moro, ACA 2015 PC Chair

and Ilias Kotsireas, ACA 2015 General Chair


Computer
Algebra
Computational
Applications
Algebraic
applications
Gröbner
quantum
information
Theory
algebra
theory
Bases
methods
Algorithmic
Rings
Non
computing
finite
complexity
Resultants
Symbolic
Basis
Topology
standard
Linear
Integral
mathematical
fields
Cryptography
difference
Polytopes
Differential
Polynomial
integration
differential
Coding
Open
Human-Computer
Operator
Interaction
Solving
Source
algorithms
Methods
System
Software
Graph
Applied
Computation
aspects
summation
Education
Matrices

General schedule

Sunday 19	17:00 – 20:00	Registration

	Monday 20				Tuesday 21				Wednesday 22				Thursday 23			
	Track 1	Track 2	Track 3	Track 4	Track 1	Track 2	Track 3	Track 4	Track 1	Track 2	Track 3	Track 4	Track 1	Track 2	Track 3	Track 4
08:00 – 09:00	Registration															
09:00 – 09:30	Opening Remarks				53 S7	54 S9	55 S10	56 S11	104 S4	105 S7	106 S13	107 S16	123 S11	124 S5	125 S4	126 S14
09:30 – 10:00	1 S1	2 S2	3 S3	4 S6	57 S7	58 S9	59 S10	60 S11	108 S4	109 S7	110 S13	111 S16	127 S11	128 S5	129 S4	130 S14
10:00 – 10:30	5 S1	6 S2	7 S3	8 S6	61 S7	62 S9	63 S10	64 S11	112 S4	113 S7	114 S13	115 S16	131 S11	132 S5	133 S4	134 S14
10:30 – 11:00	9 S1	10 S2	11 S3	12 S6	65 S7	66 S9	67 S10	68 S11	116 S4	117 S7	117 S13	118 S16	135 S11	136 S5	137 S12	138 S14
11:00 – 11:30	Break				Break				Break				Break			
11:30 – 12:00	13 S1	14 S2	15 S3	16 S6	69 S6	70 S9	71 S10	72 S11	119 S4	120 S7	121 S13	122 S16	139 S11	140 S5	141 S12	142 S14
12:00 – 12:30	17 S1	18 S2	19 S3	20 S6	Plenary Talk				Maple Talk				143 S11	144 S5	145 S12	146 S14
12:30 – 13:00	21 S1	22 S2	23 S3	24 S6									147 S11	148 S5	149 S12	150 S14

13:00 – 15:00	Lunch				Lunch				Lunch	Lunch			
15:00 – 15:30	25 S1	26 S2	27 S3	28 S6	73 S6	74 S9	75 S3	76 S11	EXCURSION Ancient Messini archaeological site	151 S11	167 S10	152 S12	153 S14
15:30 – 16:00	29 S15	30 S2	31 S3	32 S6	77 S6	78 S9	79 S3	80 S11		154 S11		155 S4	156 S14
16:00 – 16:30	33 S15	34 S5	35 S3	36 S6	81 S6	82 S9	83 S3	84 S11		157 S11		158 S4	159 S14
16:30 – 17:00	37 S15	38 S5	39 S3	40 S6	85 S6	86 S12	87 S3	88 S11		160 S11		161 S4	162 S14
17:00 – 17:30	Break				Break					163 S11		164 S4	165 S14
17:30 – 18:00	41 S15	42 S5	43 S3	44 S9	89 S6	90 S12	91 S3	92 S15		Closing Remarks			
18:00 – 18:30	45 S15	46 S5	47 S3	48 S9	93 S6	94 S13	95 S3	96 S15					
18:30 – 19:00	49 S15	50 S5	51 S3	52 S9	97 S6	98 S13	99 S3	100 S15					
19:00 – 19:30	166 S15				101 S6		102 S3	103 Hands on	Banquet				
					Business meeting								

Monday

	Monday 20			
	Track 1	Track 2	Track 3	Track 4
08:00 – 09:00	Registration			
09:00 – 09:30	Opening Remarks			
09:30 – 10:00	1 S1 A. Orlowski, From classical universal and reversible logical operations to quantum computation	2 S2 Tetsuo Fukui, S. Shirai: Predictive Algorithm from Linear String to Mathematical Formulae for Math Input Method	3 S3 Elena Varbanova About balanced application of CAS in undergraduate mathematics	4 S6 F. Winkler Birational Transformations of Algebraic Ordinary Differential Equations
10:00 – 10:30	5 S1 V. Gerdt, A. Khvedelidze, Y. Palii, On the orbit space of unitary actions for mixed quantum states	6 S2 Hans-Gert Gräbe, Albert Heinle, Simon Johannig: Symbolic Data, Computer Algebra and the Web 2.0	7 S3 F. Botana Some reflections about open vs. proprietary Computer Algebra Systems in mathematics teaching	8 S6 Christian Schilli, Eva Zerz, and Viktor Levandovskyy: Controlled and conditioned invariance for polynomial and rational feedback systems
10:30 – 11:00	9 S1 J.A. Miszczak, States and channels in quantum mechanics without complex numbers	10 S2 Joris van der Hoeven, Grégoire Lecerf, Denis Raux: Preserving Syntactic Correctness While Editing Mathematical Formulas	11 S3 Razvan A. Mezei Create SageMath Interacts for All Your Math Courses	12 S6 P. Olver Invariant histograms and signatures for object recognition, symmetry detection, and jigsaw puzzle assembly
11:00 – 11:30	Break			
11:30 – 12:00	13 S1 O.G. Karamitrou, C. Tsimpouris, P. Mavridi, K.N. Sgarbas, Web based Quantum Computer Simulator and symbolic extensions	14 S2 Manfred Minimair: Collaborative Computer Algebra: Review of Foundations	15 S3 Gregory V. Bard Using SageMathCell and Sage Interacts to Reach Mathematically Weak Business Students	16 S6 L. Poinsot Jacobi algebras, in-between Poisson, differential, and Lie algebras
12:00 – 12:30	17 S1 A. SaiToh, Practical Difficulty and Techniques in Matrix-Product-State Simulation of Quantum Computing in Hilbert Space and Liouville Space	18 S2 Manfred Minimair: Modelling Inductive Reasoning in Collaborative Computer Algebra	19 S3 Josef Böhm GINI-Coefficient, GOZINTO-Graph and Option Prices	20 S6 A. Kitchin Quantized Weyl algebras and Automorphisms
12:30 – 13:00	21 S1 A. Prokopenya, Approximate Quantum Fourier Transform and Applications: Simulation with Wolfram Mathematica	22 S2 Elena Smirnova: CAS wonderland: A journey from user interfaces to user-friendly interfaces	23 S3 M. Beaudin and F. Henri When Mathematics Meet Computer Software	24 S6 C. Raab On a generalization of integro-differential operators

13:00 – 15:00	Lunch			
15:00 – 15:30	25 S1 A. Kissinger, The ZX-calculus and quantum computation	26 S2 Laurence Ruiz Ugalde: Cooperative development and human interface of a computer algebra system with the Fōrmulæ framework	27 S3 Th. Dana-Picard and N. Zehavi Revival of a Classical Topic in Differential Geometry: Envelopes of Parametrized Families of Curves and Surfaces	28 S6 C. Shakiban Application of Signature Curves to Characterize Melanomas and Moles
15:30 – 16:00	29 S15 Zhuo-Heng He and Qing-Wen Wang, Properties and applications of a simultaneous decomposition of seven matrices over real quaternion algebra	30 S2 Stephen M. Watt: Browser-based Collaboration with InkChat	31 S3 G. Labelle Generating animations of JPEG images of closed surfaces in space using Maple and Quicktime	32 S6 M. Kauers Walks in the quarter plane with multiple steps
16:00 – 16:30	33 S15 P. Psarrakos, Travelling from matrices to matrix polynomials	34 S5 Matthias Seiss: Root parameterized differential equations for the classical groups	35 S3 David Zeitoun and Thierry Dana-Picard Plotting technologies for the study of functions of two real variables	36 S6 W. Seiler Computing Resolutions for Linear Differential Systems
16:30 – 17:00	37 S15 Tongsong Jiang and Zhaozhong Zhang, Algebraic techniques for eigenvalues of a split quaternion matrix in split quaternionic mechanics	38 S5 Alin Bostan: Quasi-optimal computation of the p-curvature	39 S3 Wlodzimierz Wojas and Jan Krupa Some remarks on Taylor's polynomials visualization using Mathematica in context of function approximation	40 S6 M. Jaroschek Computing Formal Solutions of Completely Integrable Pfaffian Systems With Normal Crossings
17:00 – 17:30	Break			
17:30 – 18:00	41 S15 Zhaozhong Zhang and Tongsong Jiang, Algebraic methods for Least Squares problem in split quaternionic mechanics	42 S5 Manuel Kauers: The positive part of multivariate series	43 S3 Jeanett López García, Jorge J. Jiménez Zamudio and Ma. Eugenia Canut Díaz Velarde Visualization of Orthonormal Triads in Cylindrical and Spherical Coordinates	44 S9 Aldo Gonzalez-Lorenzo, Fast computation of Betti numbers on three-dimensional cubical complexes
18:00 – 18:30	45 S15 Jianlong Chen, Moore-Penrose inverse and Drazin inverse of some elements in a ring	46 S5 Florian Heiderich: Prolongation spaces and generalized differentials	47 S3 R. Hasek Contemporary interpretation of a historical locus problem with an unexpected discovery	48 S9 Eduardo Sáenz de Cabezón. Computing the homology of the lcm-filtration of a monomial ideal
18:30 – 19:00	49 S15 R. Padmanabhan and Y. Zhang, Using Prover9 for proving some matrix equations	50 S5 Mohamed Barakat: Unitary groups of group algebras in characteristic 2	51 S3 Michael Xue A Constructive Proof of Feuerbach's Theorem Using a Computer Algebra System	52 S9 Darian Onchis. Estimating the position of the mandibular canal in dental radiographs using the generalized Hough transform
19:00 – 19:30	166 S15 Guang-Jing Song, Some results concerning condensed Cramers rule for the general solution to some restricted quaternion matrix equations			

Tuesday

	Tuesday 21			
	Track 1	Track 2	Track 3	Track 4
09:00 – 09:30	53 S7 Frederic Chyzak Explicit generating series for small-step walks in the quarter plane	54 S9 Marian Mrozek. Algebraic-topological invariants for combinatorial multivector fields	55 S10 Juan García Escudero The root lattice A2 in the construction of tilings and algebraic hypersurfaces with many singularities	56 S11 Christian Eder Improved Parallel Gaussian Elimination for Gröbner Bases Computations in Finite Fields
09:30 – 10:00	57 S7 Jürgen Gerhard Definite Integration of Rational Functions	58 S9 Joao Pita Costa, Mikael Vejdemo-Johansson and Primoz Skraba. Persistence over a topos of variable sets	59 S10 E. Roanes-Lozano, J.L. Galán-Garciía, G. Aguilera-Venegas Computer Algebra-based RBES personalized menu generator	60 S11 Ioannis Emiris Sparse multihomogeneous systems, root counts and discriminants
10:00 – 10:30	61 S7 Manuel Kauers Creative Telescoping via Hermite Reduction	62 S9 Vitaliy Kurlin. Fast and Stable Topological Profiles of Noisy 2D Images	63 S10 Robert H. Lewis Symbolic-Numeric Computing: A Polynomial System Arising in Image Analysis of Point Cloud Data	64 S11 Anders Jensen Tropical homotopy continuation
10:30 – 11:00	65 S7 Ngo Quoc Hoan Harmonic sums and polylogarithms at negative multiple-indices	66 S9 Gard Spreemann, Benjamin Dunn, Magnus Botnan, Yasser Roudi and Nils Baas. Using persistent homology to reveal hidden information in place cells	67 S10 M. Ramírez, J.M. Gavilán, G. Aguilera, J.L. Galán, M.Á. Galán, P. Rodríguez Making more flexible ATISMART+ model for traffic simulations using a CAS	68 S11 Matthew Niemerg Bounds on the Number of Real Solutions For a Family of Fewnomial Systems of Equations via Gale Duality
11:00 – 11:30	Break			
11:30 – 12:00	69 S6 T. Goncalves Conservation Laws and the Chazy Equation	70 S9 Grzegorz Jablonski. Persistence of generalized eigenspaces of self-maps	71 S10 P. Pech Properties of the Simson–Wallace locus applied on a skew quadrilateral	72 S11 Jean-Charles Faugere Linear Algebra for Computing Gröbner Bases of Linear Recursive Multidimensional Sequences
12:00 – 12:30	Plenary Talk Peter Olver - Algebras of Differential Invariants			
12:30 – 13:00				
13:00 – 15:00	Lunch			

15:00 – 15:30	73 S6 A. Korporal Generalized Green's Operators and the Method of Characteristics	74 S9 Mateusz Juda. Algebraic Topology For Unitary Reflection Groups - Scalable Homology Computing	75 S3 Gennadi and Nastasha Malaschonok Math Partner and Math Tutor	76 S11 Victor Pan Real Polynomial Root-finding by Means of Matrix and Polynomial Iterations
15:30 – 16:00	77 S6 E. Previato Symbolic Computation for Rankin-Cohen Differential Algebras	78 S9 Marc Ethier, Grzegorz Jabłoński and Marian Mrozek. Computing the persistence of a self-map with the Kronecker canonical form	79 S3 Michel Beaudin Ideas for Teaching Using CAS	80 S11 Elias Tsigaridas Nearly optimal algorithms for real and complex root refinement
16:00 – 16:30	81 S6 S. Maddah Formal Solutions of Singularly-Perturbed Linear Differential Systems	82 S9 Pedro Real. Exploring relationships between homology generators using algebraic-topological models of regular CW-complexes.	83 S3 Josef Böhm Solving Brain Teasers/Twisters - CAS Assisted	84 S11 SiraniPerera A Fast Euclid-type Algorithm for Quasiseparable Polynomials
16:30 – 17:00	85 S6 V. Bavula Localizable and Weakly Left Localizable Rings	86 S12 K. Chatouh, K. Guenda, T. A. Gulliver and L. Noui Simplex and MacDonald Codes over R_q	87 S3 Alkiviadis G. Akritas Various New Methods for Computing Subresultant Polynomial Remainder Sequences (PRS's)	88 S11 John Perry Midway upon the journey
17:00 – 17:30	Break			
17:30 – 18:00	89 S6 M. Barakat Generalized morphisms – turning homological algorithms into closed formulas	90 S12 Pierre-Louis Cayrel Mohammed Meziani and Ousmane Ndiaye. SBS: A Fast and Provably Secure Code-Based Stream Cipher	91 S3 G. Aguilera, J.L. Galán, M.Á. Galán, Y. Padilla, P. Rodríguez, R. Rodríguez Teaching improper integrals with CAS	92 S15 Guihai Yu, Inertia of weighted graphs
18:00 – 18:30	93 S6 T. Combot Computing Liouvillian solutions of linear difference equations	94 S13 Eleni Tzanaki - A geometric approach for the upper bound theorem for Minkowski sums of convex polytopes.	95 S3 Wlodzimierz Wojas and Jan Krupa Application of wxMaxima System in LP problem of compound feed mass minimization	96 S15 Hui Qu, More on minmum skew-rank of graphs
18:30 – 19:00	97 S6 A. Prokopenya Symbolic Computation in Studying the Restricted Three-Body Problem with Variable Masses	98 S13 Christos Konaxis - A sparse implicitisation framework	99 S3 T. Takahashi, T. Sakai, F. Iwama The Use of CAS for Logical Analysis in Mathematics Education	100 S15 XiaominTang, Post-Lie algebra structures on solvable Lie algebra t(2, C)
19:00 – 19:30	101 S6 N. Malashonok One symbolical method for solving differential equations with delayed argument		102 S3 David Jeffrey Indexed elementary functions in Maple	103 SymbolicData aspects hands on session Hans-Gert Graebe, Albert Heinle, Viktor Levandovsky
	Business meeting			

Wednesday

	Wednesday 22			
	Track 1	Track 2	Track 3	Track 4
08:00 – 09:00				
09:00 – 09:30	104 S4 M. Borges-Quintana, M.A. Borges-Trenard, E. Martínez-Moro Trial set and Gröbner bases for binary codes	105 S7 Erik Panzer Symbolic integration of multiple polylogarithms	106 S13 Winfried Bruns - Normal lattice polytopes	107 S16 D. J. Bates , D. Brake , M. Niemerg Implementation of Coefficient-Parameter Homotopies in Parallel
09:30 – 10:00	108 S4 Ryutaroh Matsumoto and Diego Ruano Geometric and Computational Approach to Classical and Quantum Secret Sharing	109 S7 Clemens Raab Algorithms in symbolic integration	110 S13 Vissarion Fisikopoulos - Enumeration of 2-level polytopes	111 S16 S. Al-Ashhab The Four Corner Magic and semi pandiagonal Squares
10:00 – 10:30	112 S4 C. Galindo, F. Hernándo, D. Ruano Quantum codes with bounded minimum distance	113 S7 Mark Round Refined Holonomic Summation Meets Particle Physics	114 S13 Christof Soeger - Recent developments in Normaliz	115 S16 A. S. Perminov, E. D. Kuznetsov Use computer algebra system Piranha for expansion of the Hamiltonian and construction averaging motion equations of the planetary system problem
10:30 – 11:00	116 S4 O. Geil, S. Martin, U. Martínez-Peñas and D. Ruano Refined analysis of RGHWs of code pairs coming from Gracia-Stichtenoth's second tower	117 S7 Carsten Schneider Refined Parameterized Telescoping Algorithms	117 S13 Anders Jensen - Starting cones for tropical traversals	118 S16 Adrian Ionescu, Rea Ulaj Use of Linux Open-Source Software and Maple in Analyzing the New Goeken-Johnson Runge-Kutta Type Methods
11:00 – 11:30	Break			
11:30 – 12:00	119 S4 M. Bras-Amorós, M.E. O'Sullivan and M. Pujol A new approach to the key equation and to the Berlekamp-Massey algorithm	120 S7 Eugene Zima Dispersion and complexity of indefinite summation	121 S13 Martin Helmer - Computing the Chern-Scwrartz-MacPherson Class and Euler Characteristic of Complete Simplical Toric Varieties	122 S16 D. Burkholder Using CAS to Uncover Unexpected Hidden Beauty in Radin-Conway's Pinwheel Tiling
12:00 – 12:30	Maple Talk Juergen Gerhard – New features in Maple 2015			
12:30 – 13:00				
13:00 – 15:00	Lunch			

15:00 – 15:30	EXCURSION Ancient Messini archaeological site
15:30 – 16:00	
16:00 – 16:30	
16:30 – 17:00	
17:00 – 17:30	
17:30 – 18:00	
18:00 – 18:30	
18:30 – 19:00	
19:00 – 19:30	Banquet

Thursday

	Thursday 23			
	Track 1	Track 2	Track 3	Track 4
08:00 – 09:00				
09:00 – 09:30	123 S11 Guenael Renault Application of Computer Algebra in Number Theory Based Cryptology	124 S5 Carlos Arreche: On the computation of the difference-differential Galois group for a second-order linear difference equation	125 S4 J. Borges, C. Fernández-Córdoba and R. Ten-Valls On Z_{p^r}Z_{p^s}-additive cyclic codes	126 S14 Gregory Bard - A Brief Introduction to the Extended Linearization Method (or XL Algorithm) for Solving Polynomial Systems of Equations.
09:30 – 10:00	127 S11 Ludo Tolhuizen The HIMMO Scheme	128 S5 Andreas Maurischat: Differential Galois theory over differentially simple rings	129 S4 R.D. Barrolleta and M. Villanueva PD-sets for (nonlinear) Hadamard Z4-Linear codes	130 S14 Jean-Charles Faugère - Gröbner Bases and Structured Systems: an Overview.
10:00 – 10:30	131 S11 Ludovic Perret Algebraic Attack against Wild McEliece & Incognito	132 S5 Thomas Dreyfus: Malher equations, differential Galois theory, and transcendence	133 S4 J. Rifà, E. Suárez-Canedo Kronecker sums to construct Hadamard full propelinear codes of type CnQ8	134 S14 Joris van der Hoeven - On the Complexity of Polynomial Reduction.
10:30 – 11:00	135 S11 Nadia El Mrabet Use of Groebner basis in order to perform a fault attack in pairing-based cryptography	136 S5 Ivan Tomasic: Primitive recursive quantifier elimination for existentially closed difference fields	137 S12 Irene Márquez-Corbella, Ruud Pellikaan A characterization of MDS codes that have an error correcting pair	138 S14 Jie Zhou - The Generalized Rabinowitsch's Trick.
11:00 – 11:30	Break			
11:30 – 12:00	139 S11 Tristan Vaccon Computation of Groebner bases and tropical Gröbner bases over $p$-adic fields	140 S5 Daniel Robertz: Lagrangian constraints and differential Thomas decomposition	141 S12 Bernhard Garn and Dimitris E. Simos Algebraic Modelling of Covering Arrays	142 S14 Anna Karasoulou - Resultant of an Equivariant Polynomial System with Respect to the Symmetric Group.
12:00 – 12:30	143 S11 Sharwan Kumar Tiwar Modular Techniques to Compute Grooebner Bases over Non-Commutative Algebras with PBW Bases	144 S5 Werner Seiler: Geometric singularities of algebraic differential equations	145 S12 Bernhard Garn and Dimitris E. Simos Algebraic Modelling of Covering Arrays	146 S14 Robert Lewis - Symbolic Solution of Parametric Polynomial Systems with the Dixon Resultant.
12:30 – 13:00	147 S11 Chun-Ming Yuan Efficient Groebner bases computation for Z[x] lattice	148 S5 148 Franz Winkler: Symbolic solution of first-order autonomous algebraic partial differential equations	149 S12 Relinde Jurrius and Ruud Pellikaan On defining generalized rank weights	150 S14 Manfred Minimair - Design of a Maple Package for Dixon Resultant Computation.
13:00 – 15:00	Lunch			

15:00 – 15:30	151 S11 Robert H. Lewis Solving Polynomial Systems Using the Dixon-EDF Resultant with Emphasis on Image Analysis Problems	167 S10 FatmaZohra Belkredim Truth Value formalization and Groups Theory	152 S12 Abdelkader Hamttat and Djilali Behloul On the diophantine equation 1 + 5x^2 = 3y^n	153 S14 Manuel Kauers - Integral Bases for D-Finite Functions.
15:30 – 16:00	154 S11 Anissa Ali An algebraic method to compute the mobility of closed-loop overconstrained mechanisms		155 S4 M. Durcheva A Message Encryption Scheme Using Idempotent semirings	156 S14 Suzy Maddah - LINDALG: Mathemagix Package for Symbolic Resolution of Linear Differential Systems with Singularities.
16:00 – 16:30	157 S11 Jinsan Cheng Solving polynomial system with linear univariate representation		158 S4 V. Berec Simplicial topological coding and homology of spin networks	159 S14 Dimitrios Poulakis - Bezout Matrices and Roots of Quaternion Polynomials.
16:30 – 17:00	160 S11 Gennadi Malaschonok About Triangular Matrix Decomposition in Domain		161 S4 Karim Ishak, Sven Muelich, Sven Puchinger, Martin Bossert Code-based Cryptosystems using generalized concatenated codes	162 S14 Elias Tsigaridas - Nearly optimal bit complexity bounds for computations with structured matrices
17:00 – 17:30	163 S11 Jérémy Berthomieu Polynomial-Time Algorithms for Quadratic Isomorphism of Polynomials:The Regular Case		164 S4 A. Jeux and C. Pierrot Nearly Sparse Linear Algebra and application to the Discrete Logarithm Problem	165 S14 Erol Yilmaz - Linear Algebraic Approach to H-Basis Computation.
17:30 – 18:00	Closing Remarks			
18:00 – 18:30				
18:30 – 19:00				
19:00 – 19:30				

Plenary Talks

Algebras of Differential Invariants

Peter Olver
Head School of Mathematics
University of Minnesota
Minneapolis, Minnesota, USA
olver@umn.edu

New features in Maple 2015

Jürgen Gerhard
Director of Research at Maplesoft, Canada
Former member of the Research Group Algorithmic Mathematics and of the MuPAD Research Group at University of Paderborn, Germany
GerhardJuergen@web.de

Computer algebra in quantum computing and quantum information theory

Session Organizers

Vladimir Gerdt
Laboratory of Information Technologies
Joint Institute for Nuclear Research Dubna
`gerdt@jinr.ru`

Michael Mc Gettrick
De Brun Centre for Computational Algebra, School of Mathematics
National University of Ireland Galway
`michael.mcgettrick@nuigalway.ie`

Jaroslaw Adam Miszczak
Institute of Theoretical and Applied Informatics
Polish Academy of Sciences Gliwice
`miszczak@iitis.pl`

Arkadiusz Orłowski and Alexander Prokopenya
Faculty of Applied Informatics and Mathematics
Warsaw University of Life Sciences
{ `arkadiuszorlowski,alexanderprokopenya` } `@sggw.pl`

Overview

Quantum information processing provides a plethora of new problems and research topics suitable for tackling using computer algebra systems. This includes the problems of characterizing multipartite entanglement, generation and optimization of quantum computational circuits and analysis of quantum walks and quantum automata. In the reverse direction, quantum algorithms which outperform their classical counterparts may be of use in symbolic calculations (e.g. Gröbner Bases).

The aims of this session are to exchange recent results and ideas concerning the application of numerical, symbolic and algebraic methods in quantum information processing and quantum mechanics.

From Classical Universal and Reversible Logical Operations to Quantum Computation

Arkadiusz Orłowski[1]

[1] *Faculty for Applied Informatics and Mathematics, University of Life Sciences - SGGW, Nowoursynowska 166, 02-787 Warszawa, Poland, arkadiusz_orlowski@sggw.pl*

Reversible logical operations implemented via reversible logic gates (that can be realized in practice, at least approximately, using various physical processes) play an important role in both low-power electronics [1, 2] and quantum computations [3]. First, reversibility of classical computational circuits helps to avoid additional energy dissipation and heat generation that is immanently tied to irreversible computation due to Landauer's principle [4]. Second, quantum gates and quantum circuits have to be reversible due to the very nature of unitary quantum evolution [5].

Here different classification schemes of reversible logical operations, including but not restricted to those obtained via group–theoretical methods, are presented for different *logic widths* of corresponding gates. Searching for universal subsets of reversible gates is undertaken with the help of computer algebra systems. New results and nontrivial observations are provided as compared to the pioneering paper [6]. Novel less-typical reversible and universal logic gates are discussed and their possible applications are suggested. Some remarks concerning *optimal* designs of reversible classical and quantum circuits are also given.

References

[1] Kalyan S. Perumalla, *Introduction to Reversible Computing*, CRC Press, Taylor & Francis Group, Boca Raton, 2014.

[2] Alexis De Vos, *Reversible Computing. Fundamentals, Quantum Computing, and Applications*, Wiley–VCH, Weinheim, 2010.

[3] Michael A. Nielsen, Isaac L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.

[4] Rolf Landauer, *Irreversibility and Heat Generation in the Computational Process*, IBM Journal of Research and Development **5** (3), 183-191 (1961).

[5] Richard Feynman, *Feynman Lectures on Computation*, Addison–Wesley Publishing, Reading, 1996.

[6] Alexis De Vos, Birger Raa, Leo Storme, *Generating the group of reversible logic gates*, Journal of Physics A: Mathematical and General **35**, 7063-7078 (2002).

On the orbit space of unitary actions for mixed quantum states

Vladimir Gerdt, Arsen Khvedelidze, Yuri Palii

Laboratory of Information Technologies,
Joint Institute for Nuclear Research,
141980 Dubna, Moscow Region, Russia
E-mail: gerdt@jinr.ru

Abstract

The space of mixed states, $\mathfrak{P}_+$, of n-dimensional binary quantum system is locus in quo for two unitary groups action: the group $\mathrm{U}(n)$ and the tensor product group $\mathrm{U}(n_1) \otimes \mathrm{U}(n_2)$, where n_1, n_2 stand from dimensions of subsystems, $n = n_1 n_2$. Both groups act on a state $\varrho \in \mathfrak{P}_+$ in adjoint manner $(\mathrm{Ad}\, g\,)\varrho = g\,\varrho\, g^{-1}$. As a result of this action one can consider two equivalent classes of ϱ; the *global* $\mathrm{U}(n)-$orbit and the *local* $\mathrm{U}(n_1) \otimes \mathrm{U}(n_2)-$orbit. The collection of all $\mathrm{U}(n)$-orbits, together with the quotient topology and differentiable structure defines the "global orbit space", $\mathfrak{P}_+ \,|\mathrm{U}(n)$, while the orbit space $\mathfrak{P}_+ \,|\mathrm{U}(n_1) \otimes \mathrm{U}(n_2)$ represents the "local orbit space", or the so-called *entanglement space* $\mathcal{E}_{n_1 \times n_2}$. The latter space is proscenium for manifestations of the intriguing effects occurring in quantum information processing and communications.

Both orbit spaces admit representations in terms of the elements of integrity basis for the corresponding ring of group-invariant polynomials. This can be done implementing the Processi and Schwarz method, introduced in the 80th of last century for description of the orbit space of a compact Lie group action on a linear space. According to the Processi and Schwarz the orbit space is identified with the semi-algebraic variety, defined by the syzygy ideal for the integrity basis and the semi-positivity condition of a special, so-called "gradient matrix", $\mathrm{Grad}(z) \geqslant 0$, constructing from the integrity basis elements.

In the present talk we address the question of application of this generic computer algebra aided approach to the construction of $\mathfrak{P}_+ \,|\mathrm{U}(n)$ and $\mathfrak{P}_+ \,|\mathrm{U}(n_1) \otimes \mathrm{U}(n_2)$. Namely, we study whether the semi-positivity of Grad$-$ matrix introduces a new conditions on the elements of the integrity basis for the corresponding ring $\mathbb{R}[\mathfrak{P}_+]^{\mathrm{G}}$.

States and channels in quantum mechanics without complex numbers

J.A. Miszczak[1]

[1] *Institute of Theoretical and Applied Informatics of the Polish Academy of Sciences, Bałtycka 5, 44-100 Gliwice, Poland, miszczak@iitis.pl*

In this work we demonstrate a simplified version of quantum mechanics in which the states are constructed using real numbers only. In the standard formulation of quantum mechanics the state is represented by positive semidefinite, normalized linear operators. In the following we focus on linearity and hermicity properties of density matrices as they are crucial for the properties of quantum channels.

The main advantage of the introduced approach is that the simulation of the n-dimensional quantum system requires $\mathcal{O}(n^2)$ real numbers, in contrast to the standard case where $\mathcal{O}(n^4)$ real numbers are required.

The main disadvantage is the lack of hermicity in the representation of quantum states. This leads to the occurrence of complex eigenvalues of the real-valued density matrices.

During the last few years *Mathematica* computing system has become very popular in the area of quantum information theory and the foundations of quantum mechanics. The main reason for this is its ability to merge the symbolic and numerical capabilities, both of which are often necessary to understand the theoretical and practical aspects of quantum mechanical systems [1, 2, 3].

We utilize the symbolic calculation capabilities offered by *Mathematica* [4, 5] to investigate the properties of the variant of quantum theory based of the representation of density matrices built using real-numbers only. We develop a set of functions for manipulating real quantum states. With the help of this tool we study the properties of the introduced representation and the induced representation of quantum channels.

We start by introducing the said representation, including the required functions. We show how it can be used in *Mathematica* using symbolic computation. Next we test the behavior of selected partial operations in this representation and we consider the general case of quantum channels acting on the space of real density matrices. Finally, we provide the summary and the concluding remarks.

Acknowledgements This work has been supported by Polish National Science Centre project number 2011/03/D/ST6/00413.

References

[1] V.P. Gerdt, R. Kragler, A.N. Prokopenya, *A Mathematica package for simulation of quantum computation*, in Computer Algebra in Scientific Computing / CASC'2009, V.P. Gerdt, E.W. Mayr, E.V. Vorozhtsov (ed.), LNCS 5743, Springer-Verlag, Berlin, pp. 106-117 (2009).

[2] J.A. Miszczak, *Generating and using truly random quantum states in Mathematica*, Comput. Phys. Commun., Vol. 183, No. 1 (2012), pp. 118-124. arXiv:1102.4598

[3] B. Julia-Diaz, *Simulating quantum computers with Mathematica: QDENSITY et al.*, In: *Proc. Applications of Computer Algebra (ACA2013)*, Malaga, 2-6 July 2013, J.L. Galan Garcia, G. Aguilera Venegas, P. Rodriguez Cielos, (eds.), 2013.

[4] J.A. Miszczak, *Singular value decomposition and matrix reorderings in quantum information theory*, Int. J. Mod. Phys. C, Vol. 22, No. 9 (2011), pp. 897-918. arXiv:1011.1585

[5] J.A. Miszczak, *Functional framework for representing and transforming quantum channels*, In: *Proc. Applications of Computer Algebra (ACA2013)*, Malaga, 2-6 July 2013, J.L. Galan Garcia, G. Aguilera Venegas, P. Rodriguez Cielos, (eds.), 2013. arXiv:1307.4906

A Web-based Quantum Computer Simulator with symbolic extensions

O. G. Karamitrou[1], C. Tsimpouris[2], P. Mavridi[3], K. N. Sgarbas[4]

[1] *University of Patras, Greece, okaramitrou@upatras.gr*
[2] *University of Patras, Greece, xtsimpouris@upatras.gr*
[3] *University of Patras, Greece, petramauridi@gmail.com*
[4] *University of Patras, Greece, sgarbas@upatras.gr*

The objective of this paper is to present a quantum computer simulator with a web interface based on the circuit model of quantum computation [3]. This is the standard model for which most quantum algorithms have been developed. Quantum algorithms are expressed as circuits of quantum registers (series of qubits) and quantum gates operating on them. Each quantum gate is a unitary transformation on the Hilbert space determined by the quantum register.

The quantum computer simulator is developed in Python, using some extra libraries for our purposes. The fundamental library that is used is Numpy: the package for scientific computing with Python.

Because of the limitations of GUI for a large number of qubits, we propose an another version of quantum computer simulator without a user interface, which could simulate quantum computations for larger inputs. The inputs of the simulator are the number of qubits, the number of computation steps, the initial state of quantum register and the gates that applied at each step. The outputs of the simulator are the quantum register state at each step (the probability of measuring each one of the possible states and the phases of each state).

The quantum computer simulator is a useful tool for studying and understanding quantum circuits, quantum computations and well known quantum algorithms such as Grover's algorithm [1, 2] and Quantum Fourier Transform. It may also be very useful for the development of new quantum algorithms and the construction of new quantum gates.

Another approach of developing a quantum simulator in Python, is to use instead of Numpy, Sympy python library (Symbolic Python). The advantage of this change is that you can represent very large numbers, as a result of using arbitrary precision arithmetic. On the other hand, Numpy uses machine arithmetic, which imports limitations.

References

[1] L. K. Grover, *Quantum mechanics helps in searching for a needle in a haystack*, Phys. Rev. Lett. **79**, 2, pp. 325-328 (1997).

[2] L. K. Grover, *Quantum computers can search rapidly by using almost any transformation*, Phys. Rev. Lett. **80**, 19, pp. 4329-4332 (1998).

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge, U.K.:Cambridge University Press, (2000).

Practical Difficulty and Techniques in Matrix-Product-State Simulation of Quantum Computing in Hilbert Space and Liouville Space

Akira SaiToh[1]

[1] *Toyohashi University of Technology, Toyohashi, Aichi, Japan, saitoh@cs.tut.ac.jp*

There have been many studies on matrix-product-state (MPS) simulation of quantum computing for more than a decade [1, 2, 3, 4, 5, 6]. Although it is widely believed to be unlikely, it is still an open problem if a practical simulation of a powerful quantum algorithm like Shor's factoring algorithm is possible. This situation is owing to the fact that not only theoretical analyses but numerical investigations on MPS are quite cumbersome.

In practice, coding an MPS simulation program is highly technical. A quantum circuit should be carefully decomposed as its structure affects the Schmidt ranks of MPS during simulation. In addition, numerical error may accumulate rapidly if we use only double-precision floating-point arithmetics because almost always we need to diagonalize highly degenerate reduced density matrices during simulation. Furthermore, sometimes quantum states initially having very small population play an important role in an algorithm. Thus, multiple-precision computing is often requisite to obtain a reasonable simulation result [5, 6].

In this contribution, I summarize the above-mentioned issues with explicit examples, and how I have been coding my open source C++ library, ZKCM_QC [5, 6]. I also discuss the simulability of spin-Liouville-space quantum computations on the basis of some simulation results.

References

[1] G. Vidal, *Efficient classical simulation of slightly entangled quantum computations*, Phys. Rev. Lett. **91**, 147902 (2003).

[2] A. Kawaguchi, K. Shimizu, Y. Tokura, and N. Imoto, *Classical simulation of quantum algorithms using the tensor product representation*, arXiv:quant-ph/0411205 (2004).

[3] M. C. Bañuls, R. Orús, J. I. Latorre, A. Pérez, and P. Ruiz-Femenía, *Simulation of many-qubit quantum computation with matrix product states*, Phys. Rev. A **73**, 022344 (2006).

[4] A. SaiToh and M. Kitagawa, *Matrix-product-state simulation of an extended Brüschweiler bulk-ensemble database search*, Phys. Rev. A. **73**, 062332 (2006).

[5] A. SaiToh, *A multiprecision C++ library for matrix-product-state simulation of quantum computing: Evaluation of numerical errors*, J. Phys.: Conf. Ser. **454**, 012064 (2013).

[6] A. SaiToh, *ZKCM: A C++ library for multiprecision matrix computation with applications in quantum information*, Comput. Phys. Comm. **184**, pp.2005-2020 (2013).

Approximate Quantum Fourier Transform and Applications: Simulation with Wolfram Mathematica

Alexander N. Prokopenya

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

The quantum Fourier transform (QFT) is a unitary transformation U_{FT} that can be written in the computational basis $|x\rangle_n \equiv |x_{n-1}\dots x_1 x_0\rangle$, where the set of numbers $x_j = 0,1$ $(j = 0,1,\dots,n-1)$ provides the binary representation of the integer x $(x = 0,1,...,2^{n-1})$, as

$$U_{FT}|x\rangle_n \to \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} \exp\left(\frac{2\pi i}{2^n} xy\right) |y\rangle_n \, . \tag{1}$$

Here n is a number of qubits in the memory register.

Note that the QFT can be carried out efficiently by a quantum circuit built entirely out of single-qubit and two-qubit gates. Actually, only n the Hadamard gates, $n(n-1)/2$ controlled phase shift gates R_k, and $\lfloor n/2 \rfloor$ Swap gates are required to build such a circuit (see, for example, [1]). The execution time of the QFT grows only as n^2 and, therefore, the QFT is executed exponentially faster that the classical fast Fourier transform.

However, in case of a large number of qubits the phase shift $2\pi/2^k$ becomes exponentially small, while a practical implementation of the high precision controlled phase shift gates R_k may be very difficult. So it would be very useful if the full Fourier transform (1) could be replaced by the approximate QFT, where only finite degree phase shift gates R_k are involved $(k \leq m < n)$. Analysis of different quantum algorithms has shown that applying the approximate QFT can yield even better results than the full Fourier transform [2].

In the present paper we discuss an approximate QFT that was first proposed in [3] and can be represented as

$$\begin{aligned}\tilde{U}_{FT}|x_{n-1}\dots x_0\rangle \to \frac{1}{2^{n/2}} \sum_{y_{n-1}=0}^{1} \dots \sum_{y_0=0}^{1} \exp\Big(2\pi i \Big(x_{n-1}\frac{y_0}{2} + \dots +\\ x_{n-m}\left(\frac{y_{m-1}}{2^1} + \dots + \frac{y_0}{2^m}\right) + x_{n-m-1}\left(\frac{y_m}{2^1} + \dots + \frac{y_1}{2^m}\right) + \dots +\\ x_0\left(\frac{y_{n-1}}{2^1} + \dots + \frac{y_{n-m}}{2^m}\right)\Big)\Big) |y_{n-1}\dots y_0\rangle \, .\end{aligned} \tag{2}$$

Applying the approximate QFT, one can expect that an accuracy of computation decreases in comparison to the case of the full QFT, and probability of getting a correct result reduces, as well. The main purpose of the present paper is to estimate a probability of successful solution of a problem in case of the replacement of the full QFT by the approximate QFT and to demonstrate the results by simulation of some quantum algorithms, using the Wolfram Mathematica package "QuantumCircuit" (see [4, 5]). Recall that the package provides a user-friendly interface to specify a quantum circuit, to draw it, and to construct the corresponding unitary matrix for quantum computation defined by the circuit. Using this matrix, one can find the final state of the quantum memory register by its given initial state and to check the operation of the algorithm determined by the quantum circuit.

As examples we consider here two known quantum algorithms, where the QFT plays an essential role. The first one is the quantum algorithm for phase estimation based on the QFT [6]. We have obtained the lower bound on the probability of the successful phase estimation in both cases of the full and approximate QFT and shown that the decrease in the accuracy of phase estimation results in increasing the probability of the successful problem solution [7].

The second example is the Shor algorithm for order finding [8]. Our calculations show that using the approximate QFT gives the same results as in case of the full QFT even for small enough degree m of approximation. At the same time the probability to obtain correct result decreases only a little bit in comparison to the case of the full QFT. The validity of the results is demonstrated by simulation of the algorithm using the package "QuantumCircuit".

References

[1] M. Nielsen, I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000).

[2] A. Barenco, A. Ekert, K.A. Suominen, P. Törmä, *Approximate quantum Fourier transform and decoherence*, Phys. Rev. A

[3] D. Coppersmith, *An approximate Fourier transform useful in quantum factoring*, IBM Research Report RC 19642 (1994). **54**, 1, pp.139-146 (1996).

[4] V.P. Gerdt, R. Kragler, A.N. Prokopenya, *A Mathematica program for constructing quantum circuits and computing their unitary matrices*, Physics of Particles and Nuclei, Lett. **6**, 7, pp. 526-529 (2009).

[5] V.P. Gerdt, R. Kragler, A.N. Prokopenya, *A Mathematica package for simulation of quantum computation*, in *Computer Algebra in Scientific Computing / CASC'2009*, V.P. Gerdt, E.W. Mayr, E.V. Vorozhtsov (ed.), LNCS 5743, Springer-Verlag, Berlin, pp. 106-117 (2009).

[6] D.S. Abrams, S. Lloyd, *Quantum algorithm providing exponential speed increase for finding eigenvales and eigenvectors*, Phys. Rev. Lett. **83**, 24, pp. 5162-5165 (1999).

[7] A.N. Prokopenya, *Simulation of a quantum algorithm for phase estimation*, Programming and Computer Software **41**, 2, pp. 98-104 (2015).

[8] P.W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comp. **26**, 5, pp. 1484-1509 (1997).

The ZX-calculus and quantum computation

Aleks Kissinger[1]

[1] *University of Oxford, UK, alek@cs.ox.ac.uk*

The ZX-calculus is a formal system for reasoning diagrammatically about quantum computation which admits an encoding of the circuit model and measurement-based quantum computation. In this talk, I'll give an introduction to the calculus itself, survey some of the most important theorems, techniques, and open problems, and demonstrate the implementation of the ZX-calculus in Quantomatic, a diagrammatic proof assistant.

Human-Computer Algebra Interaction

Session Organizers

Manfred Minimair
Department of Mathematics and Computer Science
Seton Hall University
minimair@shu.edu

Stephen M. Watt
Computer Science Department
The University of Western Ontario
watt@uwo.ca

Overview

This session explores how humans interact with computer algebra software to solve problems in applications and research. The topics for presentations include software to support cooperative work in computer algebra, mathematical experimentation, specialized user interfaces and hardware to increase productivity, such as software wizards, mobile devices, and pen-based input, and applications to artificial intelligence. The session intersects with the 2009 session on Applications of Math Software to Mathematical Research and the 2005 session on Pen-Based Mathematical Computing.

Predictive Algorithm from Linear String to Mathematical Formulae for Math Input Method

T. Fukui[1], S. Shirai[2]

[1] *Mukogawa Women's University, Japan, fukui@mukogawa-u.ac.jp*
[2] *Mukogawa Women's University, Japan, shirai@mukogawa-u.ac.jp*

1 Introduction

In recent years, Computer Aided Assessment (CAA) systems have been used for mathematics education. A few CAA systems enable users to directly input mathematical expressions to allow their answers to be evaluated automatically by using a computer algebra system (CAS). These systems have also been used to provide instruction to students at universities. However, the procedure according to which an answer is entered into the system by using the standard input method for mathematics is still troublesome [1, 2].

In 2011, Professor Tetsuo Fukui of Mukogawa Women's University proposed a new mathematical input method for conversion from a colloquial style mathematical text[3]-[7]. This method is similar to those used for inputting Japanese characters in many operating systems. In this system, the list of candidate characters and symbols for the desired mathematical expression, as obtained from the user input, is displayed in WYSIWYG format and once all the elements the user wishes to include are chosen, then the expression formatting process is complete. This method will enable the user to input almost any mathematical expression without having to learn a new language or syntax. However, the disadvantage of the abovementioned method is that the user has to convert each element contained in the colloquial style mathematical string by proceeding from left to right, in this order.

This study aimed to address this shortcoming by improving the math input efficiency using an intelligently predictive conversion from a linear mathematical string to an entire expression instead of converting each element individually.

2 Linear String rules

The linear mathematical string rules for a mathematical expression are described as follows:

> Set the key letters (or words) corresponding to the elements of a mathematical expression linearly in the order of colloquial (or reading) style, without considering two-dimensional placement and delimiters.

In other words, a key letter (or word) consists of the ASCII code(s) corresponding to the initial or the clipped form (such as the LaTeX-form) of the objective mathematical symbol. Therefore, one key often supports many mathematical symbols. For example, when a user wants to input α^2, the linear string is denoted by “a2" where “a" stands for the “alpha” symbol and it is unnecessary to include a power sign (such as the caret letter (ˆ)). In the case of $\frac{1}{\alpha^2+3}$, the linear string is denoted by “1/a2+3" where it is not necessary to surround the denominator (which is generally the operand of an operator) by parentheses, because they are never printed.

3 Design of intelligently predictive conversion

In this talk, we propose a predictive algorithm to convert a linear string s into the most suitable mathematical expression y_p. For prediction purposes, we devised a method by which each candidate for selection would be ranked in terms of its suitability. Our method uses a function $\mathrm{Score}(y)$ to allocate a score which is proportional to the probability of a mathematical expression y occurring, and which would enable us to predict the candidate y_p by eq.(1) as being the most suitable expression with the maximum score. Here, $Y(s)$ in eq.(1) is the totality of all the possible mathematical expressions converted from s.

$$y_p \ \text{ s.t. } \ \mathrm{Score}(y_p) = \max\{\mathrm{Score}(y) | y \in Y(s)\} \tag{1}$$

A mathematical expression consists of mathematical symbols, namely numbers, variables, or *operators* [1], together with the operating relations between a specific operator and an element. Therefore, we decided to represent a mathematical expression by a tree structure consisting of nodes and edges corresponding to the symbols and operating relations, respectively.

First, all the node elements of mathematical expressions were classified according to nine types, as listed in Table 1 in this math conversion system. Therefore, a node element is characterized by (k,e,t) where k is the key letter (or word) of its mathematical symbol e that belongs to type $t(=N,V,P,A,B_L,B_R,C,Q,R$, or $T)$ in Table 1. For example, the number 2 is characterized by $(\text{“2"},2,N)$ and similarly a variable x by $(\text{“x"},x,V)$ and, as for the Greek letter α, it can either be characterized by $(\text{“alpha"},\alpha,V)$ or $(\text{“a"},\alpha,V)$. In the case of the operator, the character $(\text{“/"},\frac{\triangle_1}{\triangle_2},C)$ represents a fractional symbol with input key “/", where $\triangle_1,\triangle_2$ represents arbitrary operands.

There are 510 mathematical symbols and the 597 operators in the node element table $\mathscr{D}$ implemented by our prototype system in this study.

[1] In this article, "operator" is used in the sense of operating on, i.e., performing actions on elements in terms of their arrangements for two-dimensional mathematical notation.

Table 1: Nine types of mathematical expressive structures

Math element	Codes of type	examples ($\triangle_1, \triangle_2, \triangle_3$ represent operands)
Number	N	$2, 128$
Variable, Symbol	V	x, α
Prefix unary operator	P	$\sqrt{\triangle_1}, \sin \triangle_1$
Postfix unary operator	A	$\triangle_1'$
Bracket	B_L, B_R	$(\triangle_1)$
Infix binary operator	C	$\triangle_1 + \triangle_2, \frac{\triangle_1}{\triangle_2}$
Prefix binary operator	Q	$\log_{\triangle_1} \triangle_2$
Prefix ternary operator	R	$\int_{\triangle_1}^{\triangle_2} \triangle_3$
Infix ternary operator	T	$\triangle_1 \overset{\triangle_2}{\to} \triangle_3$

The totality $Y(s)$ of mathematical expressions converted from s is calculated by the following procedures (Proc. 1)-(Proc. 3) referring to the node element table $\mathscr{D}$.

(Proc. 1) A linear string s is separated in the group of keywords defined in eq.(2) by using the parser in this system.

$$s = k_1 \uplus k_2 \uplus \cdots k_K \text{ where } (k_i, v_i, t_i) \in \mathscr{D}, i = 1, ..., K \tag{2}$$

(Proc. 2) Predictive expressive structures are fixed by analyzing the group of keywords and comparing the nine types of structures in Table 1.

(Proc. 3) From the fixed structures corresponding to the operating relations between the nodes, we obtain $Y(s)$ by applying all the possible combinations of math elements belonging to each keyword in $\mathscr{D}$.

4 Predictive Algorithm

Let us assume that the probability of a certain math element occurring is proportional to the score depending on its frequency of use. Then, the probability of occurrence of a mathematical expression y, which is possibly converted from a given string s, is estimated by the total of the scores of all the elements included in y. Given the numbering of each element from 1 to F_{total}, which is the total number of all elements, let θ_f be the score of the $f(= 1, \cdots, F_{total})$-th element and let $x_f(y)$ be the number of the f-th element included in y. Then, Score(y) in eq.(1) is estimated by eq.(3) where score vector $\theta^T = (\theta_1, \cdots, \theta_{F_{total}})$ and F_{total}-dimensional vector $X = (x_f(y)),\ f = 1, \cdots, F_{total}$.

$$h_\theta\left(X(y)\right) = \theta^T \cdot X(y) = \sum_{f=1}^{F_{total}} \theta_f x_f(y) \tag{3}$$

Eq.(3) is in agreement with the hypothesis function of linear regression and $X(y)$ is referred to as the characteristic vector of y. To solve our linear regression problem and predict the probability of a mathematical expression occurring, we have planned supervised machine learning by m number of a training dataset $\{(s_1,y_1),(s_2,y_2),\cdots,(s_m,y_m)\}$. Our learning algorithm for the optimized score vector is performed by the following procedure from (Step 1) to (Step 4).

(Step 1) Initialization: $\theta = 0$, $i = 1$

(Step 2) Decision of a candidate: y_p s.t. $h_\theta\left(X(y_p)\right) = \max\{h_\theta\left(X(y)\right) | y \in Y(s_i)\}$

(Step 3) Training parameter: if($y_p \neq y_i$) {

$$\begin{array}{lll} \theta_f := \theta_f + 1 & \text{for} & \{{}^\exists f \leq F_{total} | x_f(y_i) = 1\} \\ \theta_{\bar{f}} := \theta_{\bar{f}} - 1 & \text{for} & \{{}^\exists \bar{f} \leq F_{total} | x_{\bar{f}}(y_p) = 1\} \end{array} \tag{4}$$

}

(Step 4) if($i \leq m$){ i=i+1; go to Step 2 for repetition.}
else { Output θ and end.}

This learning algorithm is very simple, and is similar to machine learning by structured perceptron in natural language processing[9].

5 Experimental evaluation

We have examined the prediction accuracy using two parameter sets of score learning from an evaluation dataset contained in 800 mathematical formulae which are printed in a textbook of mathematics[8]. The two parameter sets of θ for scoring are trained by two kinds of algorithm, respectively, that are programed in Java on a desktop computer (MacOS 10.9, 3.2 GHz Intel core i3, 8 GB memory) as follows.

Algorithm 1 (Step 1)–(Step 4) in eq.(4).

Algorithm 2 (Step 1)–(Step 4) that exchanged (Step 3) with the following eq.(5).

$$\begin{array}{lll} \theta_f := \theta_f + 2 & \text{for} & \{{}^\exists f \leq F_{total} | x_f(y_i) = 1\} \\ \theta_{\bar{f}} := \theta_{\bar{f}} - 1 & \text{for} & \{{}^\exists \bar{f} \leq F_{total} | x_{\bar{f}}(y_p) = 1\} \end{array} \tag{5}$$

In this experimental evaluation, we observed the ratios of predictions that were answered correctly among the 100 test datasets after learning the parameters with each of Algorithms 1 and 2 by using a training dataset consisting of another 700 formulae.

The machine learning result with Algorithm 1 is given in Table 2 for each training number. It shows that the accuracy of "Best 1" becomes about 79.1% after being trained 700 times. In the top ten ranking ("Best 10"), it achieves about 89.2%.

On the other hand, the result obtained by using Algorithm 2 with another learning weight is given in Table 3. The prediction accuracy of "Best 1" becomes about 68.5% after being trained 700 times. It achieves about 95.0% in the top ten ranking, which is sufficient for a math input interface system. However, we remark that the score parameter continues to rise while Algorithm 2 is undergoing learning and this will be improved in our future work.

Table 2: Prediction accuracy by Algorithm 1

training number	Best1 (%)	(SD)	Best3 (%)	(SD)	Best10 (%)	(SD)
0	25.9	3.8	41.3	4.4	52.3	4.3
100	62.7	14.7	75.5	9.2	81.5	6.8
200	75.6	6.6	82.7	5.0	86.6	4.3
300	79.3	4.1	85.2	4.3	88.1	4.3
400	79.2	3.8	85.1	3.8	88.2	3.5
500	80.0	4.4	86.7	4.0	89.5	3.3
600	79.5	3.7	85.9	3.4	89.2	3.8
700	79.1	5.7	85.7	5.3	89.2	4.2

Table 3: Prediction accuracy by Algorithm 2

training number	Best1 (%)	(SD)	Best3 (%)	(SD)	Best10 (%)	(SD)
0	25.9	3.8	41.3	4.4	52.3	4.3
100	53.3	14.6	82.5	6.4	88.5	4.3
200	60.3	5.0	86.1	4.2	91.7	3.2
300	64.1	5.1	89.1	3.2	93.8	2.9
400	67.7	5.7	90.1	3.1	94.1	3.1
500	67.6	5.7	90.6	2.9	94.5	2.8
600	69.1	4.6	90.8	2.7	94.3	2.5
700	68.5	6.0	91.1	2.5	95.0	2.5

6 Conclusion and Future work

We propose a predictive algorithm in terms of a structured perceptron in natural language processing. We have examined the prediction accuracy using two parameter sets of score learning from an evaluation dataset containing 800 mathematical formulae from a textbook of mathematics. The results show that the accuracy with the first of our proposed algorithms approaches 79.1%. In the top ten ranking, it achieves about 89.2%. On the other hand, the accuracy obtained with the second algorithm approaches 68.5% and it achieves about 95.0% in the top ten ranking. The mean real time for prediction per mathematical expression was approximately 623 milliseconds (SD = 819).

Finally, we expect many users' experience in terms of math input efficiency to be improved using our proposed predictive algorithm. The most important avenues for future research are to shorten the time for prediction and develop an intelligent math input interface system by implementing our proposed predictive algorithm.

This work was supported by JSPS KAKENHI Grant Number 26330413.

References

[1] M. Pollanen, T. Wisniewski, and X. Yu, *XPRESS: A Novice Interface for the Real-Time Communication of Mathematical Expressions*, In Proceedings of MathUI2007 (2007).

[2] C.J. Sangwin, *Computer Aided Assessment of Mathematics Using STACK*, in *Proceedings of ICME*,**12** (2012).

[3] T. Fukui, *An Intelligent Method of Interactive User Interface for Digitalized Mathematical Expressions(in Japanese)*, RIMS Kokyuroku, **1780**, pp.160-171 (2012).

[4] T. Fukui, *The performance of interactive user interface for digitalized mathematical expressions using an intelligent formatting from linear strings(in Japanese)*, RIMS Kokyuroku, **1785**, pp.32-44 (2012).

[5] T. Fukui, *An Intelligent User Interface Technology for Easy Formatting of Digitalized Mathematical Expressions – a Mathematical Expression Editor on Web-Browser –(in Japanese)*, Interaction 2013 IPSJ Symposium Series, **2013**, No.1, 2EXB-50, pp.537-540 (2013).

[6] S. Shirai and T. Fukui, *Development and Evaluation of a Web-Based Drill System to Master Basic Math Formulae Using a New Interactive Math Input Method*, International Congress on Mathematical Software 2014, Lecture Notes in Computer Science 8592, Springer, pp.621-628 (2014).

[7] S. Shirai and T. Fukui, *Improvement in the Input of Mathematical Formulae into STACK using Interactive Methodology (in Japanese)*, Computer & Education **37**, pp.85-90 (2014).

[8] H. Matano, the other 28, *Mathematics I*, **001**, TOKYO SHOSEKI (2012).

[9] C. D. Manning and H. Scheutze, *Foundations of Statistical Natural Language Processing*, The MIT Press, London (2012).

SymbolicData, Computer Algebra and Web 2.0

H.-G. Gräbe[1], A. Heinle[2], S. Johanning[3]

[1] *Leipzig University, Germany, graebe@informatik.uni-leipzig.de*
[2] *University of Waterloo, Canada, aheinle@uwaterloo.ca*
[3] *Leipzig University, Germany, simonjohanning@googlemail.com*

1 Introduction

What is Computer Algebra (CA)? Twenty years ago more than 200 leading edge computer algebraists in a worldwide joint effort compiled a description of the CA landscape [4] and defined the target of CA in the following way:

> "Computer Algebra is a subject of science devoted to methods for solving mathematically formulated problems by symbolic algorithms, and to implementation of these algorithms in software and hardware. It is based on the exact finite representation of finite or infinite mathematical objects and structures, and allows for symbolic and abstract manipulation by a computer. Structural mathematical knowledge is used during the design as well as for verification and complexity analysis of the respective algorithms. Therefore computer algebra can be effectively employed for answering questions from various areas of computer science and mathematics, as well as natural sciences and engineering, provided they can be expressed in a mathematical model." [4, p. 2]

Johannes Grabmeier, at that time head of the German CA Fachgruppe, developed an even broader view of a subject *Computer Mathematics* as a symbiosis of computer technology and mathematics at large as the true core of "Scientific Computing" [5]. Such a *technology*[1] *of quantitative methods* is a corner stone of any science, that "can be considered as developed"[2]. Figure 1 displays these concepts, the difference between deductive and numerical mathematics and the position of such a *Computer Mathematics* between mathematics and computer science.

Twenty years later a practical incarnation of such a vision is any of the mature General Purpose Computer Algebra Systems, in particular the one that claims to be "the world's definitive system for modern technical computing" [9].

[1] Technology considered in the broad sense of *applicable processual knowledge* in the ancient greek meaning, see e.g., [16], not in the narrow meaning of *tool, tool making, tool using* as, e.g., in the German VDI-3780 norm [17].

[2] A claim attributed to Karl Marx by Paul Lafargue. David Hilbert supports such a view: "Everything that can be an object of scientific thinking as soon as it matures to formation of theories is in the bondage of the axiomatic method and thus indirectly of mathematics." [8]

What remained from such an integrated view – a *CA Tower of Babel* – twenty years later? What is the relation between the sections of ACA 2015, that address specialized and over the years even more and more specialized topics? What are the consequences of a division of CA into more and more sub- and subsubcommunities? Has THE LORD confused their language[3] once more?

2 The SYMBOLICDATA Project

2.1 The Roots

SYMBOLICDATA hab been part of CA infrastructural efforts for more than 15 years. It grew up from the Special Session on Benchmarking at the 1998 ISSAC conference, and started to build a reliable and sustainably available reference of Polynomial Systems data, to extend and update it, to collect meta information about the records, and also to develop tools to manage the data and to set up and run testing and benchmarking computations on the data. The main design decisions and implementations of the first prototype were realized by Olaf Bachmann and Hans-Gert Gräbe in 1999 and 2000. We collected data from *Polynomial Systems Solving* and *Geometry Theorem Proving*, set up a CVS repository, and started test computations with the main focus on Polynomial Systems Solving.

In 2005 the Web site `http://www.symbolicdata.org` sponsored by the German CA Fachgruppe went online and a second phase of active development started. Data was supplied by the CoCoA group (F. Cioffi), the Singular group (M. Dengel, M. Brickenstein, S. Steidel, M. Wenk), V. Levandovskyy (non commutative polynomial systems, G-Algebras) and Raymond Hemmecke (Test sets from Integer Programming). During the Special Semester on Groebner Bases in March 2006 we discussed aspects to extend the project, in particular with Bruno Buchberger, Alexander Zapletal, and Viktor Levandovskyy.

2.2 Version 3 – SYMBOLICDATA Goes Semantic

A third phase started in 2009 when the project joined forces with the Agile Knowledge Engineering and Semantic Web (AKSW) Group at Leipzig University [1] in order to strongly refactor the data along standard Semantic Web concepts based on the Resource Description Framework (RDF) [15]. In 2012–2014 these efforts were

[3] But the Lord came down to see the city and the tower which the sons of men had built. And the Lord said, "Indeed the people are one and they all have one language, and this is what they begin to do; now nothing that they propose to do will be withheld from them. Come, let Us go down and there confuse their language, that they may not understand one another's speech." (Genesis 11)

supported by a 12 month grant for Andreas Nareike and another 5 month grant for Simon Johanning within the *Saxonian E-Science Initiative* [3].

Within this scope we completed a redesign of the data along the rules of Linked Data and semantic, RDF-based technology, distinguishing more consequently between data (*resources* in the RDF terminology) and meta data (*knowledge bases* in the RDF terminology). The new SymbolicData data and tools were released as version 3.0 in September 2013. Version 3.1 is to be released in the mid of 2015.

Resources (examples for testing, profiling and benchmarking software and algorithms from different CA areas) are publicly available (mainly) in XML markup, meta data in RDF notation both from a public git repo, hosted at `github.org`, and from an OntoWiki based RDF data store at `http://symbolicdata.org/Data`. Moreover, we offer a SPARQL endpoint to explore the data by standard Linked Data methods.

The website operates on a standard installation using an Apache web server to deliver the data, a Virtuoso RDF data store as data backend, a SPARQL endpoint and (optionally) OntoWiki to explore, display and edit the data. This standard installation can easily be rolled out on a local site (tested under Linux Debian and recent Ubuntu versions; a more detailed description can be found in our wiki [14]) to support local testing, profiling and benchmarking.

The distribution offers also tools for integration with a local computational environment as, e.g., provided by Sagemath [13] – the Python based *SDEval package* [7] by Albert Heinle offers a JUnit-like framework to set up, run, log, monitor and interrupt testing and benchmarking computations, and the *sdsage package* [10] by Andreas Nareike provides a showcase for SymbolicData integration with the Sagemath computational environment.

Currently the SymbolicData data collection contains resources from the areas of Polynomial Systems Solving (390 records, 633 configurations), Free Algebras (83 records), G-Algebras (8 records), GeoProofSchemes (297 records) and Test Sets from Integer Programming (49 records).

Note that such a concept is not restricted to resources centrally managed at `symbolicdata.org`, but can easily be extended to other data stores on the web that are operated by different CA subcommunities and offer a minimum of Linked Data connectivity. There are draft versions of resource descriptions about Fano Polytopes (8630 records) and Birkhoff Polytopes (5399 records) from the `polymake` project hosted by Andreas Paffenholz and about Transitive Groups (3605 records) from the Database for Number Fields of Jürgen Klüners and Gunter Malle that point to external resources. For Test Sets we joined forces with the Normaliz group — Tim Römer provided some new benchmarks and refactored the old examples to fit with the `normaliz` syntax.

2.3 The Vision: Towards a Computer Algebra Social Network

I come back to the *CA Tower of Babel* image unfolded in the introduction. If we shift the focus of any project – and we did so for SymbolicData with version 3.0 – from the *data* to the *people and their intentions* perspective – *why* they collect and manipulate such data – new organizational perspectives for common efforts are revealed. The business of any CA project is a techno-social one and we think in the spirit of sociomateriality [12], it is time to use the *technical means* of a semantically enriched Web 2.0 to also strengthen the *social* part of our cooperation and to contribute to the efforts to build up an interconnected *E-Science World*.

During the last years such efforts matured within the *Science at Large*. Services such as MathSciNet, arXiv.org, or EasyChair.org have been established and their usefulness is widely acknowledged. There are plenty of new activities, in particular by the *national libraries and organizations* [18], by the *Zentralblatt Mathematik* [11], or by the IMU, that advances the vision of a *21st Century Global Library for Mathematics Research* (GDML) [2].

It is a great challenge to smaller scientific communities to adopt such developments for their own scientific communication processes and to join forces with other scientific communities to get own requirements publicly recognised. A first step in such a direction could be a more detailed description of ongoing scientific processes using standard RDF terminology.

With version 3 SymbolicData started to address the technical aspects of such cooperational needs in more detail, developed a vision of a *Computer Algebra Social Network* (CASN) [6], and started to realize it.

3 About our Talk

In this abstract we tried to explain the background of our project and in particular the data services available to the public. We operate these services on a stable basis, but the current focus of the project is on the CASN concepts and the difficult (social) task to get them running. In our presentation at ACA 2015 we will concentrate on a report about the current state of our efforts towards such a CASN. To prepare for our talk we invite interested people to look at our project wiki [14] and in particular at the survey paper [6].

We expect fruitful discussions and hope to convince more people that such a project is not only a “nice to have” but also deserves own *practical* efforts. The train is ready for departure. Don’t miss it!

References

[1] The Agile Knowledge Engineering and Semantic Web Group at Leipzig University, `http://aksw.org/About.html` [2014-02-19].

[2] *Developing a 21st Century Global Library for Mathematics Research. Report of the Committee on Planning a Global Library of the Mathematical Sciences*, The National Academies Press (2014).

[3] The eScience Research Network Saxony, `http://www.escience-sachsen.de` [2014-02-19].

[4] J. Grabmeier, E. Kaltofen, V. Weispfenning (eds.), *Computer Algebra Handbook. Foundations – Applications – Systems*, Springer Verlag, Berlin (2003).

[5] J. Grabmeier, *Computeralgebra – eine Säule des Wissenschaftlichen Rechnens*, it + ti, **6:5**, p. 20 (1995).

[6] H.-G. Gräbe, S. Johanning, A. Nareike, *The* SYMBOLICDATA *Project – from Data Store to Computer Algebra Social Network*, Computeralgebra Rundbrief, vol. **55**, pp. 22–26 (2014), see also `http://symbolicdata.org/Papers/car-55.pdf` [2015-04-12].

[7] A. Heinle, V. Levandovskyy, *The SDEval Benchmarking Toolkit*, Communications in Computer Algebra, vol. **49.1**, pp. 1–10 (2015), see also `http://wiki.symbolicdata.org/SDEval` [2015-04-12].

[8] Citation from `http://de.wikipedia.org/wiki/Wissen` [2015-04-11], attributed to Hermann Weyl, *Philosophie der Mathematik und Naturwissenschaft*, R. Oldenbourg, Munich (1976).

[9] `http://www.wolfram.com/mathematica/` [2015-04-11]

[10] A. Nareike, *The* SYMBOLICDATA *sdsage package*, `http://wiki.symbolicdata.org/PolynomialSystems.Sage` [2015-04-12].

[11] U. Schöneberg, W. Sperber, *POS Tagging and its Applications for Mathematics*, in *Intelligent Computer Mathematics*, LNCS vol. 8543, pp. 213–223 (2014).

[12] Sociomateriality, see `http://en.wikipedia.org/wiki/Wanda_Orlikowski` [2015-04-12].

[13] Sage – a free open-source mathematics software system, `http://www.sagemath.org` [2014-02-19].

[14] The SYMBOLICDATA Project Wiki, `http://wiki.symbolicdata.org` [2015-04-12].

[15] J. Tauberer, *Quick Intro to RDF*, `http://www.rdfabout.com/quickintro.xpd` [2014-02-20].

[16] Technology, `http://en.wikipedia.org/wiki/Technology` [2015-04-11].

[17] DIN Deutsches Institut für Normung e.V., *VDI 3780 – Technology Assessment Concepts and Foundations*, VDI-Richtlinie, ed. 2000-09.

[18] VIAF: Virtual International Authority File. `https://viaf.org/` [2015-04-12].

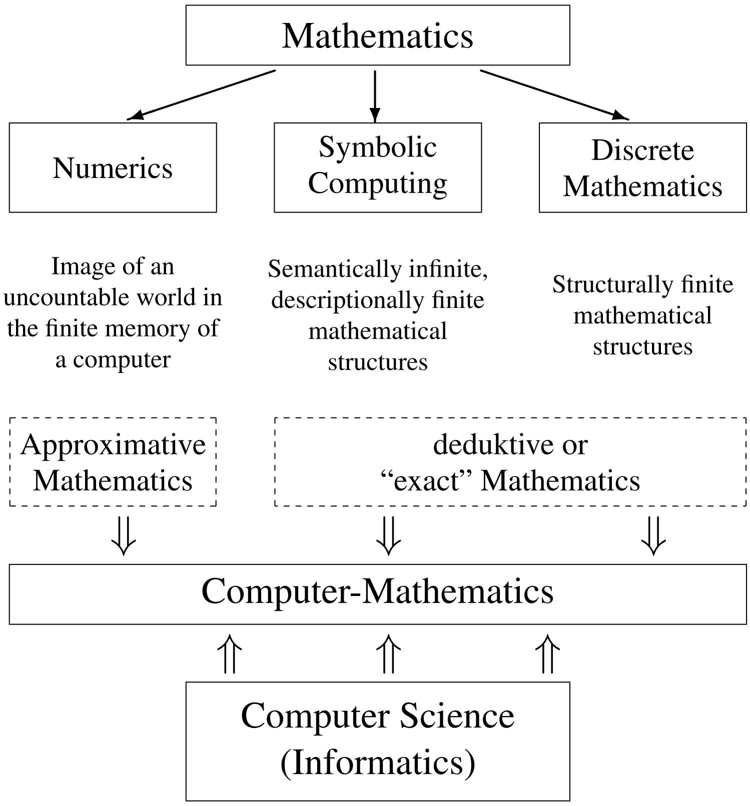

Mathematics
Numerics
Symbolic Computing
Discrete Mathematics
Image of an uncountable world in the finite memory of a computer
Semantically infinite, descriptionally finite mathematical structures
Structurally finite mathematical structures
Approximative Mathematics
deduktive or "exact" Mathematics
Computer-Mathematics
Computer Science (Informatics)

Figure 1: The Genesis of Computermathematics

Preserving syntactic correctness while editing mathematical formulas

Joris van der Hoeven[a], Grégoire Lecerf[b], Denis Raux[c]

Laboratoire d'informatique, UMR 7161 CNRS
Campus de l'École polytechnique
1, rue Honoré d'Estienne d'Orves
Bâtiment Alan Turing, CS35003
91120 Palaiseau, France

a. *Email:* vdhoeven@lix.polytechnique.fr
b. *Email:* lecerf@lix.polytechnique.fr
c. *Email:* raux@lix.polytechnique.fr

May 31, 2015

Most mathematical formulas in current scientific papers only carry very poor semantics. For instance, consider the two formulas $f(x+y)$ and $a\,(b+c)$. These formulas are typically entered using the LATEX pseudo-code `$f(x+y)$` and `$a(b+c)$`. Doing so, we do not transmit the important information that we probably meant to apply f to $x+y$ in the first formula and to multiply a with $b+c$ in the second one. The problem to automatically recover such information is very hard in general. For this reason, it would be desirable to have mathematical authoring tools in which it is easy to write formulas which systematically carry this type of information.

One important application where semantics matters is computer algebra. Popular computer algebra systems such as Mathematica and Maple contain formula editors in which it is only possible to input formulas which can at least be understood from a syntactic point of view by the system. However, these systems were not really designed for writing scientific papers: they only offer a suboptimal typesetting quality, no advanced document preparation features, and no support for more informal authoring styles which are typical for scientific papers.

The GNU TEXMACS editor was designed to be a fully fledged *wysiwyg* alternative for TEX/LATEX, as well as an interface for many computer algebra systems. The software is free and can be downloaded from

http://www.texmacs.org

Although formulas only carried barely more semantics than LATEX in old versions of TEXMACS, we have recently started to integrate more and more semantic editing features. Let us briefly discuss some of the main ideas behind these developments; we refer to [6] for more details and historical references to related work.

First of all, we are only interested in what we like to call "syntactic semantics". In the formula $2+3$, this means that we wish to capture the fact that $+$ is an infix operator with arguments 2 and 3, but that we are uninterested in the fact that + stands for addition on integers. Such syntactic semantics can be modeled adequately using a formal grammar. Several other mathematical formula editors are grammar-based [1, 2, 3, 7, 9, 10], and they make use of various kinds of formal grammars. In TeXmacs, we have opted for so called *packrat* grammars [4, 5], which are particularly easy to implement and customize.

A second question concerns the precise grammar that we should use to parse formulas in scientific documents. Instead of using different grammars for various areas with different notations, we were surprised to emperically find out that a well-designed "universal" mathematical grammar is actually sufficient for most purposes; new notations can still be introduced using a suitable macro mechanism.

The last main point concerns the interaction between the editor and the grammar. So far, we implemented a packrat parser for checking the correctness of a formula. While editing a formula, its correctness is indicated using colored boxes. It is also possible to detect and visualize the scopes of operators through the grammar. In addition to the parser, we implemented a series of tools which are able to detect and correct the most common syntactic mistakes and enhance existing documents with more semantics.

In the present paper, we wish to go one step further and enforce syntactic correctness throughout the editing process. Ideally speaking, the following requirements should be met:

- As far as user input is concerned, there should be no essential difference between editing formulas with or without the new mechanism for preserving syntactic correctness. For instance, we do not wish to force users to provide additional "annotations" for indicating semantics. It should also be possible to perform any editing action which makes sense from the purely visual point of view.
- The implementation should be as independent as possible from the actual grammar being used. In other words, we strive for a generic approach, not one for which specific editing routines are implemented for each individual grammar symbol.

The main technique that we will use for sticking as closely as possible to the old, presentation oriented editing behaviour is to automatically insert "transient" markup for enforcing correctness during the editing process. For instance, when typing x+, TeXmacs will display

$$x+\square$$

The transient box is used to indicate a missing symbol or subexpression and will be removed as soon as the user enters the missing part.

The use of transient boxes for missing symbols or subexpressions is common in other editors [8]. The question which interests us here is how to automatically insert such markup when needed in a way that is essentially independent from specific grammars. In this paper, we work out the following approach which was suggested in [6]: before and after each editing operation, subject the formula to suitable "correction" procedures that are only allowed to add or remove transient markup. Correcting all errors in a general formula is a very difficult problem, but the power of our approach comes from the fact that the editing process is incremental: while typing, the user only introduces small errors—mostly incomplete formulas—, which are highly localized; we may thus hope to deal with all possible problems using a small number of "kinds of corrections".

Obviously, the simplest kinds of corrections are adding or removing a transient box at the current cursor position. This is indeed sufficient when typing simple formulas such as $x+y+z$, but additional mechanisms are needed in other situations. For instance, in the formula $\alpha+|\beta$ (with the cursor between the "+" and the "β"), entering another + results in $\alpha+\square+\beta$ (instead of $\alpha++\square\beta$ or $a++b$). Hitting backspace in the same formula $\alpha+|\beta$ yields $\alpha+\beta$; in this case, the transient "+" should be parsed as an infix addition, and not as an ordinary symbol (as was the case for a transient box).

The appropriate corrections are not always so simple. For instance, consider the quantified expression $\forall x, \exists y, P(x,y)$. Just after we entered the existential quantifier "∃", the formula will read $\forall x, \exists\square,\square$, i.e. it was necessary to add three transient symbols in order to make the expression syntactically correct. The fact that our approach should apply to general scientific documents with mathematical formulas raises several further problems. For instance, in the formula

$$a^2+b^2=c^2,$$

the trailing ponctuation "," is incorrect from a mathematical point of view, but needed inside the surrounding English sentence. Similarly, more work remains to be done on the most convenient way to include English text inside formulas while maintaining syntactic correctness.

Yet another difficulty stems from the implementation: one needs to make sure that the necessary corrections take place after *any* kind of editing operation. However, for efficiency reasons, it is important to only run the correction procedures on small parts of the document. Inside an existing editor such as TeXmacs, these requirements turn out to be quite strong, so some trade-offs may be necessary.

In what follows, we report on our first implementation of these ideas inside TeXmacs. We describe and motivate the current design, discuss remaining problems, and outline directions for future improvements. Of course, more user feedback will be necessary in order to make the new mechanisms suitable for widespread use.

References

[1] O. Arsac, S. Dalmas, and M. Gaëtano. The design of a customizable component to display and edit formulas. In *ACM Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation, July 28–31*, pages 283–290. 1999.

[2] Y. Bertot. The CtCoq system: design and architecture. *Formal Aspects of Computing*, 11(3):225–243, 1999.

[3] P. Borras, D. Clement, Th. Despeyroux, J. Incerpi, G. Kahn, B. Lang, and V. Pascual. Centaur: the system. *SIGSOFT Softw. Eng. Notes*, 13(5):14–24, 1988.

[4] B. Ford. Packrat parsing: a practical linear-time algorithm with backtracking. Master's thesis, Massachusetts Institute of Technology, September 2002.

[5] Bryan Ford. Packrat parsing: simple, powerful, lazy, linear time. In *Proceedings of the seventh ACM SIGPLAN international conference on Functional programming*, ICFP '02, pages 36–47. New York, NY, USA, 2002. ACM Press.

[6] J. van der Hoeven. Towards semantic mathematical editing. *JSC*, 71:1–46, 2015.

[7] N. Kajler. *Environnement graphique distribué pour le calcul formel*. PhD thesis, Université de Nice-Sophia Antipolis, 1993.

[8] L. Padovani and R. Solmi. An investigation on the dynamics of direct-manipulation editors for mathematics. In A. Asperti, G. Bancerek, and A. Trybulec, editors, *Mathematical Knowledge Management*, volume 3119 of *Lect. Notes Comp. Sci.*, pages 302–316. Springer Berlin Heidelberg, 2004.

[9] N. M. Soiffer. *The Design of a User Interface for Computer Algebra Systems*. PhD thesis, University of California at Berkeley, 1991.

[10] L. Théry, Y. Bertot, and G. Kahn. Real theorem provers deserve real user-interfaces. *SIGSOFT Softw. Eng. Notes*, 17(5):120–129, nov 1992.

Collaborative Computer Algebra: Review of Foundations

M. Minimair[1]

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

Introduction: The objective is to review the foundations of Collaborative Computer Algebra. Collaborative work involving computer algebra in research, applications and education is known to be very common. The reviewed foundations include software supporting collaboration in computer algebra and theoretical frameworks from human-computer interactions. The concept of Collaborative Computer Algebra has been informally introduced by Manfred Minimair at the conference Applications of Computer Algebra (ACA) 2014 [1], without providing a definition. Therefore, subsequently, a definition is proposed.

Software Supporting Collaboration in Computer Algebra: Software supporting collaboration is abundant. Computer algebra systems provide shells, worksheets and active mathematical documents that can be shared for command execution. Databases with mathematical information are used for benchmarking and knowledge management [2]. Tools from open source software development are used to collaboratively build computer algebra software. At the software infrastructure level, the Symbolic Computation Software Composability Protocol (SCSCP) [3] allows to connect different mathematical software products.

Proposed Definition and Significance: Collaborative Computer Algebra is concerned with designing, evaluating, and applying cyber-human systems (CHS), systems consisting of humans and software, for collaboratively conducting computer algebra. Therefore, Collaborative Computer Algebra can be viewed as descending from "Symbolic and algebraic manipulation" and from "Collaborative and social computing" in the 2012 ACM Computing Classification System [4]. CHS supporting computer algebra are of significance because they include highly capable software, some including techniques from artificial intelligence and machine learning [5], for solving difficult mathematical problems. They allow humans to off-load challenging cognitive tasks onto software and enable humans to transcend their individual capabilities by meshing human intelligence with software capabilities and artificial intelligence.

Human-Computer Interaction: Frameworks, including Distributed Cognition [6], Activity Theory [7] and Actor-Network Theory [8], used in human-computer interaction studies are applicable to collaborative computer algebra. Connectivism [9, 10], a more recently emerged collection of ideas, proposed as a new learning theory for the networked age, may also provide guidance for the investigation of collaborative computer algebra.

Discussion: The proposed definition of Collaborative Computer Algebra naturally leads to the complementary questions: What is the state of the art of this area? What are the open problems? A non-exhaustive list of open issues includes designing collaboration systems that support the whole process of computer algebra work, from mathematical discoveries, algorithm design, implementation, evaluation and documentation to applications, creating groupware to facilitate working groups common in computer algebra practice, and incorporating emerging Web technologies, such as Semantic Web.

References

[1] M. Minimair, *Collaborative Computer Algebra Systems*, presented at the Applications of Computer Algebra (ACA) 2014, Fordham University, The Bronx, New York (09-Jul-2014).

[2] A. Heinle and V. Levandovskyy, *The SDEval Benchmarking Toolkit*, ACM Commun Comput Algebra, **49**, 1, pp. 1–9, (2015).

[3] S. Linton, K. Hammond, A. Konovalov, C. Brown, P. W. Trinder, H.-W. Loidl, P. Horn, and D. Roozemond, *Easy composition of symbolic computation software using SCSCP: A new Lingua Franca for symbolic computation*,J. Symb. Comput, **49**, pp. 95–119, (2013).

[4] Association for Computing Machinery, *The 2012 ACM Computing Classification System* [Online]. Available: http://www.acm.org/about/class/class/2012. [Accessed: 14-Aug-2014].

[5] Z. Huang, M. England, D. Wilson, J. H. Davenport, L. C. Paulson, and J. Bridge, *Applying Machine Learning to the Problem of Choosing a Heuristic to Select the Variable Ordering for Cylindrical Algebraic Decomposition*, in *Intelligent Computer Mathematics*, S. M. Watt, J. H. Davenport, A. P. Sexton, P. Sojka, and J. Urban, Eds. Springer International Publishing, pp. 92–107, (2014).

[6] J. Hollan, E. Hutchins, and D. Kirsh, *Distributed Cognition: Toward a New Foundation for Human-computer Interaction Research*, ACM Trans Comput-Hum Interact, **7**, 2, pp. 174–196, (2000).

[7] B. A. Nardi, *Studying context: A comparison of activity theory, situated action models, and distributed cognition*, Context Conscious. Act. Theory Hum.-Comput. Interact., pp. 69–102, (1996).

[8] B. Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford; New York: Oxford University Press, (2007).

[9] G. Siemens, *Connectivism: A learning theory for the digital age*, Int. J. Instr. Technol. Distance Learn., **2**, 1, pp. 3–10 (2005).

[10] S. Downes, *Learning Networks and Connective Knowledge*, in *Collective Intelligence and E-Learning 2.0: Implications of Web-Based Communities and Networking*, H. H. Yang and S. C.-Y. Yuen (eds.), IGI Global (2010).

Modeling Inductive Reasoning in Collaborative Computer Algebra

M. Minimair[1]

[1] *Seton Hall University, South Orange, Manfred.Minimair@shu.edu*

Introduction: The objective is to provide a testable formal model of inductive reasoning by cyber-human systems (CHS), systems consisting of humans and software, collaboratively engaged in computer algebra. Inductive reasoning means generalizing insights from examples, and this work models inductively obtained knowledge how to compute mathematical objects. The ability to reason inductively has been recognized as a main determining factor for human intelligence and its importance for problem solving, learning and gaining experience has been established [1, 2]. Inductive reasoning fundamentally drives progress in science, including mathematics, because it enables to derive conjectures from observations, which, upon acceptance, become building blocks of theories. The overarching motivation is to contribute to the theoretical foundations of collaborative work in computer algebra and to eventually elucidate design principles for collaboration software based on the theoretical foundations.

Method: Inductively obtaining knowledge how to compute mathematical objects is interpreted as function finding which is fundamental in mathematics and requires cognitive skills generally applied to inductive reasoning. The developed model is based on research literature [2] describing function finding experiments in cognitive science, outcomes from computer supported collaborative learning [3] and connective knowledge [4] of CHS.

Results: An experimental scheme is proposed that generalizes data collection procedures of cognitive science for inductive reasoning of individuals to CHS. Furthermore, inductively obtained knowledge how to compute mathematical objects is formalized by an asynchronous message passing model. The knowledge, observable from the input and output behavior of the CHS, is derived as the extremal object in a category of equivalence classes of distributed algorithms. It is shown that testable conjectures can be formulated within this model.

Discussion: Connectivism [5] has been proposed as a new learning theory for the networked age. The framework of connective knowledge [4], part of connectivism, postulates that CHS obtain knowledge in a way similar to learning by artificial neural networks [6]. In particular, it is postulated that the interactions in the CHS stabilize in analogy to converging connection weights during training of artificial neural networks. The proposed formal model supports this analogy because, by learning a distributed algorithm, the interactions of the CHS are matched to the prescribed messages passed by the learned algorithm, which may be interpreted as convergence. Connectivism has been criticized for lacking testability [7] and therefore this work contributes to the foundations of connectivism by specifying a testable model of inductive reasoning. Future work includes collecting data and refining the proposed model, investigate the relationship between the CHS' and their participants' knowledge, and elucidating implications for collaboration software design.

References

[1] K. J. Klauer and G. D. Phye, *Inductive Reasoning: A Training Approach*, Rev. Educ. Res., **78**, 1, pp. 85–123 (2008).

[2] L. A. Haverty, K. R. Koedinger, D. Klahr, and M. W. Alibali, *Solving inductive reasoning problems in mathematics: not-so-trivial pursuit*,' Cogn. Sci., **24**, 2, pp. 249–298 (2000).

[3] G. Stahl, *Studying virtual math teams*, vol. 11., Springer (2009).

[4] S. Downes, *Learning Networks and Connective Knowledge*, in *Collective Intelligence and E-Learning 2.0: Implications of Web-Based Communities and Networking*, H. H. Yang and S. C.-Y. Yuen (eds.), IGI Global (2010).

[5] G. Siemens, *Connectivism: A learning theory for the digital age*, Int. J. Instr. Technol. Distance Learn., **2**, 1, pp. 3–10 (2005).

[6] G. F. Marcus, *The algebraic mind: Integrating connectionism and cognitive science*, MIT press (2003).

[7] F. Bell, *Connectivism: Its place in theory-informed research and innovation in technology-enabled learning*,' Int. Rev. Res. Open Distance Learn., **12**, 3, pp. 98–118 (2010).

CAS wonderland: A journey from user interfaces to user-friendly interfaces

Elena Smirnova[1]

[1] *Education Technology, Texas Instruments Inc. e-smirnova@ti.com*

What are the ingredients of a *good* Computer Algebra System?

1. Computational power
2. Coverage of problem set
3. Accuracy and reliability of the results
4. Ease of use
5. $\langle$ name your own $\rangle$

Depending on whom you talk to (a scientist, an educator, a student, a product marketer), the importance of the "ease of use" may supersede the other three items.

Indeed, what is good about a system that is capable of computing a determinant of a 50×50 symbolic matrix in a split of a second, if it takes half an hour to enter that matrix and then another five minutes to find out an appropriate syntax for the corresponding command?

This brings us to a discussion about two major aspects of "user interfaces" to math systems:

1. how to enter the contents (e.g. math expressions)
2. how to access system tools (e.g. math commands)

Let us try to find out what techniques are available to the users to make their experience with Computer Algebra Systems, especially those deployed on hand-held devices (i.e. missing a native hardware keyboard) more intuitive and less frustrating.

Cooperative development and human interface of a computer algebra system with the Fōrmulæ framework

Laurence R. Ugalde[1]

[1] *Fōrmulæ project founder, laurence@formulae.org*

Cooperative development of a computer algebra system (CAS) with the Fōrmulæ framework is based in modularity, it is, by the independent development of pieces that can be published, final users can choose and download a set of them and finally inserted in a base system, in which these modules can dynamically interoperate with others. Such these modules could be written by different people, places and times. There should not be required that these people or teams be managed by a central instance, instead they write programs based on a specification.

Traditionally, creating a CAS is much like creating a programming language. It must be previously fully designed and this process involves the creation of its grammar. All the programs or snippets created for such that language must be compliant with the syntax in order to be compiled or run, and since the creation of the program is usually given as code in form of text, parsers are needed in order to check the text against the grammar.

In the Fōrmulæ framework there is no a formal syntax, so there is no grammar. Every structure is dynamically defined, even the basic ones, like numbers, symbols, statements, etc.

The Fōrmulæ framework provides a set of specificaions for writing interoperable modules in three different aspects: *visualization*, *edition* and *reduction*.

Visualization

An immediate benefit of modular pieces of code is provided for visualization. There are expressions with different form of visualization, and none of them is preferable to other because the decision depends on the field of application, personal preference or even localization (i.e. the sine function in Spanish is abbreviated as *sen* (from *seno*). Two o more ways of visualization can be downloaded and installed and the user could choose which of them he or she wants to use, for example, there could be two independent modules for programming, one is intended to show programming elements as a flowchart, and the other one to show elements in a traditional, indented list of statements.

Visualization is performed in a graphic style, the expressions are shown in a pretty-print fashion which is more natural and close to how human are accustomed. for example, instead of showing the following piece of text such like

`(-b+sqrt(b^2-4*a*c))/(2*a)`, the expression can be seen in a natural way as:

$$\frac{-b+\sqrt{b^2-4ac}}{2a} \tag{1}$$

Edition

Usually, the input for a CAS session is provided as a text line, which has to be parsed for syntax verification before it could be processed. Sometimes its syntax is so complex that several CAS and/or programming languajes have been informally qualified as *write-only languages*.

Under Fōrmulæ framework, the input is always an expression, the building of a particular input is a process of tranforming an expression, adding, replacing or removing subexpressions, so no parsing is needed. An expression is always well formed. It strongly relies on the *null* expression. This simple expression resembles the zero in our numeral system, it means none by itself, but it provides structure on the positional nature and its discovery represents a great historical advance for humankind.

As an example, suppose there is a simple expression, a number:

$$5 \tag{2}$$

Then, there is the intention of creating an addend for this expression, say another number. By any method the addition operation is performed (choosing from a menu, pushing a button, pressing the '+' key, etc.) It must be impossible to create the following *pseudo* expression:

$$5+ \tag{3}$$

Instead the following is obtained. The square is used here to represent the *null expression*.

$$5+\Box \tag{4}$$

Finally, the null expression is selected, and by any other method the second number is created, which replaces the currently selected expression (the null expression) leaving the the result:

$$5+2 \tag{5}$$

By this simple method is possible to create complex expressions, in a way that in every step, the expression being built is always well formed.

Reduction

Reduction is a tranformation of an expression to another one, usually simpler, which is considered more useful. Reduction is also modular, and no exclusive, that is, a given kind of expression can have zero, one or multiple reducers associated to it.

As a very simple example, the expression $2+3$ can be transformed (o reduced) to the expression 5 because there is a reducer associated with the *addition* expression -among other reducers associated to this- that *knows* how to sum numeric addends.

As a second example, the following expression is syntactically valid:

$$\frac{the\ mars\ planet}{the\ Hg\ chemical\ element} \tag{6}$$

But it surely will not be transformed in another expressions because it is very improbable that a developer had the intention of writing a reducer for it that makes sense, because the expression has no sematic validity.

Every computable operation can be written as a reducer, and there is an algorithm for apply a set of relevant reducers in order to transform complex expressions, it is called *the reduction engine* and it is implemented as part of the Fōrmulæ framework. Most of the functionality commonly provided for known CAS are able to be written as reduction modules.

New modules can appear in order to improve the older ones -in a schema of evolution-, or to add new ways of reduction. As an example, the Risch algorithms [1] is a method for mechanical calculation of antiderivates (for a wide range of mathematical functions). In a certain point it requires a particular solution of the constant problem, that is, to test if a certain expression is equal to zero. This problem is under certain circumstances undecidable, so the effectiviness of the Risch algorithm depends of the ability to solve -formally or heuristically- the constant problem for a specific expression. Several new or impoved methods of solution of the constant problem can emerge as reduction modules that can be added to the base system, making our method of symbolic integration dynamically and gradually stronger.

Implications

It opens new possibilities for interoperate with different paradigms in a single CAS, i.e. talking about programming, since someone can write modules for different programming paradigms, it is possible to build programs or snippets with a mixture of styles, such as structured, object oriented, functional, declarative, logical, parallel, etc. Other solutions can be transported to such an interoperable methodology, for example, proof assistants and theorem provers.

There are certain computing science implications, the dynamic nature of defining, creating and implement functionality implies a creation of a ontology (a dynamic one) and it also affects the known methods of representation and transfer or knowledge

According to the results of Kurt Gödel and Alan Turing, there cannot exist a both complete and consistent system for fundamental mathematics and computability. Going further, Gregory Chaitin [2] asserts that the concept of *truth* is not absolute, it could either change with time, be sometimes random and even be accidental. In consecuence, as it is impossible to eventually create a complete/consistent monolithic CAS, we must start to focus on dynamic, cooperative methods of developement.

References

[1] R. H Risch, *The problem of integration in finite terms*, pp. 167-189 (1969).

[2] Gregory Chaitin, *Meta Math! The Quest for Omega*, (2005).

Browser-Based Collaboration with InkChat

Stephen M. Watt

University of Waterloo, Canada smwatt@uwaterloo.ca

We present the elements of a new architecture for computer-assisted mathematical collaboration based on a shared virtual canvas. Free-hand pen input, geometric sketches, typed input and images can be entered and viewed simultaneously by multiple participants. In particular, this allows the shared entry and manipulation of mathematics and the annotation of documents. Pen input is captured as InkML, rather than as raster graphics, allowing semantic analysis and manipulation. Unlike previous work, we make the communications layer fundamental and base composition and editing functions on top of that, instead of viewing communication as an add-on to a drawing program. Based on our past experience, we have chosen this time to make ease of casual use and adoption the principal design criterion. This has led to a JavaScript browser implementation and cloud-based storage.

Computer Algebra in Education

Session Organizers

Alkis Akritas
University of Thessaly
akritas@uth.gr

Michael Wester
University of New Mexico
wester@math.unm.edu

Michel Beaudin
ETS, Canada
Michel.Beaudin@etsmtl.ca

José Luis Galán García
Universidad de Málaga
jlgalan@uma.es

Elena Varbanova
Technical University of Sofia
elvar@tu-sofia.bg

Overview

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

- the commercial "heavy weights" such as Casio ClassPad 330, Derive, Magma, Maple, Mathematica, MuPAD, TI NSpire CAS, and TI Voyage 200, and
- the free software/open source systems such as Axiom, Euler, Fermat, wxMaxima, Reduce, and the rising stars such as GeoGebra, Sage, SymPy and Xcas (the swiss knife for mathematics).

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

About balanced application of CAS in undergraduate mathematics

E. Varbanova

Technical University of Sofia, Bulgaria, elvar@tu-sofia.bg

In the methodology of mathematics teaching and learning [6] the main question is "Why?". It is about the learning outcomes and educational goals as well as about educational values. The chain of questions "What-When-Where-How" is also associated with it. On one side, they can be related to the curricula and courses. On the other side, they are mostly relevant to the teaching-learning-assessment (TLA) process. In the past two-three decades remarkable creative work with application of CAS has been done in undergraduate mathematics concerning these four questions. The care about the Why-question will never end because the world constantly changes. CAS is full of opportunity in this direction as well: for adequate decisions about this question.

In this paper educational goals and values of the TLA of undergraduates mathematics [2, 4] are considered. Based on examples [1, 5] the necessity of balanced application of CAS in education is discussed. The idea is to make what is important CAS supported [3], rather than what is CAS supported important.

References

[1] T. Arens, Hettlich, F., Karpfinger, Ch., Kockelkorn, U., Lichtenegger, K. & Stachel, H. *Mathematik*, Heidelberg, Spektrum (2008).

[2] S. Grozdev, *For High Achievements in Mathematics. The Bulgarian Experience (Theory and Practice)*, Sofia, ADE (2007).

[3] E. Varbanova, *CAS supported environment for learning and teaching Calculus*, CBMS - Issues in Mathematics Education: Enhancing University Mathematics, vol. 14, AMS & MAA (2007).

[4] E. Varbanova, *Calculus - I. Lecture Notes*, Sofia, TU-Sofia (2009) (in Bulgarian).

[5] E. Varbanova, *Calculus - I. Exercises*, TU-Sofia. (2011) (in Bulgarian).

[6] G. Ganchev, Ninova, Yu., Nikova, V. *Methodology of mathematics education*, Blagoevgrad, SWU "Neofit Rilski" (2007) (in Bulgarian).

Some reflections about open vs. proprietary Computer Algebra Systems in mathematics teaching

F. Botana

University of Vigo, Spain, webs.uvigo.es/fbotana

The talk will describe some personal reflections and experiences on using Computer Algebra Systems (CAS) for undergraduate mathematics teaching. I discuss the reasons behind my transition from using proprietary CAS to Sage for mathematics teaching purposes. Problems on this transition coming from the student and institution sides are considered.

Special attention is given to Wolfram|Alpha and Sage Cell. Both applications are web-based, suitable to use in small devices. Issues on accessibility, equity and student empowerment are discussed when selecting the teaching tool.

Create SageMath Interacts for All Your Math Courses

Razvan A. Mezei[1]

[1] *Lenoir-Rhyne University, Hickory, NC, USA, razvan.mezei@lr.edu*

SageMath is a Free Open Source Software that is quickly gaining popularity in many areas of Mathematics. It has a very easy to learn Python-like syntax and gives you access to many open source packages such as: NumPy, SciPy, R, and other. One can freely download and use SageMath from their own computer, or can choose to use it over the Cloud (*SageCell* and *SageCloud* are two great options).

In this talk the presenter will talk about the use of SageMath for various Mathematics courses, for both Graduate and Undergraduate level. He will demonstrate how one can use SageMath as a rich *Computer Algebra System* (for College Algebra, Calculus, Abstract Algebra, Number Theory, etc), as a *programming tool* (for implementing Numerical Methods) or as a great *interactive software* (create SageMath interacts to demonstrate various Mathematics concepts).

References

[1] G. A. Anastassiou and Razvan A. Mezei, *NUMERICAL ANALYSIS USING SAGE*, to appear Springer 2015.

[2] Razvan A. Mezei, *An Introduction to SAGE Programming: with Applications to SAGE Interacts for Numerical Methods*, submitted 2015.

[3] William A. Stein et al., Sage Mathematics Software (Version 6.5), The Sage Development Team, 2015, http://www.sagemath.org.

Using SageMathCell and Sage Interacts to Reach Mathematically Weak Business Students

Gregory V. Bard[1]

[1] *University of Wisconsin—Stout, Wisconsin, USA, bardg@uwstout.edu*

In addition to a "business calculus" course, it is frequently required that students in business, economics, marketing, finance, accounting, and management take a course called *Finite Mathematics* in the USA, or *Quantitative Methods* in the UK. These courses often cover an assortment [1] of topics, including financial mathematics, combinatorics/probability/statistics, and problem solving with systems of linear equations, matrices, Gaussian elimination, and linear programming.

The topics of modeling with systems of linear equations and linear programming (systems of linear inequalities) are often traumatic for these students, who have weak mathematical skills, poor study habits, and little motivation. This talk will highlight some successful strategies that the speaker has used in teaching *Finite & Financial Mathematics* at the University of Wisconsin—Stout, a polytechnic located in the midwestern USA. In particular, the use of the computer algebra Sage [6], in two forms, was tremendously successful. Sage is the free and open-source competitor to Maple, Mathematica, Matlab, and Magma. Because Sage costs nothing to use, it is attractive for use in this present era of general fiscal distress worldwide.

At the start of the class's exploration of systems of linear equations/inequalities, a Sage "Interact" (a kind of app or interactive webpage) is used to model an industrial situation. To paint a clear picture, it is useful to describe this one "interact" in full detail at this time. An old factory is to be decommissioned, and a final production run will be ordered to consume as much as is possible of existing dangerous supplies. Any unused supplies must be disposed of resulting in disposal fees which might be catastrophically expensive. The students can move sliders to find a production schedule that must not use more supplies than actually exist, but that hopefully uses up "a lot" of the dangerous supplies. Usually a room full of 40 students, each experimenting on a laptop, will have a range of solutions resulting in disposal fees of around 5,000,000 to 500,000 dollars. Then a linear system of equations in four variables can be derived by the instructor, which solves the problem exactly—and which results in disposal fees of 0 dollars. The students see that knowing how to solve a system of linear equations will save the company between 500,000 and 5,000,000 dollars, and this makes them motivated to pay attention

[1] For a syllabus, see `http://www.uwstout.edu/mscs/upload/MATH-123.pdf` as an example.

during the start of this critical chapter. The reader is now invited to experiment with this interact, to be found at [1], before reading further in this abstract.

After such an introduction, students will begin to read solutions of longer problems, and then attempt to solve problems on their own. Typical American textbooks will have problems of two, three, and at most four variables during these two topics (systems of linear equations and linear programming) [3], [4], [5], [7]. The problems often are unrealistic, with "round numbers" to facilitate solving the problems by hand. In stark contrast to this, the speaker uses detailed problems with realistic numbers, many variables, and many equations/inequalities. Those would be unpleasant or nearly impossible to solve by hand. However, using SageMathCell, the systems can be easily solved. Moreover, SageMathCell works through the webbrowser[2], and therefore the students do not need to install anything.

During this talk, the speaker will present the above example, and then two or three other examples used in his teaching. The result of using computer algebra tools in this manner is that the course is transformed from focusing on the mechanical actions of performing Gaussian Elimination and the Simplex Method into one where students read complex problems, and then must model the problems as a system of equations or system of inequalities. While challenging, modeling industrial and commercial phenomena is more intellectual and a better preparation for the modern workplace.

While the speaker is not in a position to run a controlled experiment to prove the efficacy of these teaching methods, there have been several benefits in his own classroom. The students are more engaged, more likely to attempt the homework problems, they score higher on examinations, and they give the instructor better teaching evaluations. Moreover, the faculty members of the College of Management at the speaker's university have gone from expressing grave concerns to praising the mathematics department.

References

[1] G. Bard, *A Production Problem: Shutting down a Solvents Factory.* An Interactive Applet powered by Sage and MathJax. (2013).

`http://www.gregorybard.com/interacts/solvent_factory.html`

[2] G. Bard, and J. Bertino. *Applied Finite & Financial Mathematics for University Freshmen*. A textbook in progress.

`http://www.gregorybard.com/finite.html`

[3] R. Barnett, M. Ziegler, and K. Byleen. *College Mathematics for Business, Economics, Life Sciences and Social Sciences*. 12th ed. Pearson/Prentice Hall. (2010).

[2] `https://sagecell.sagemath.org/`

[4] L. Goldstein, D. Schneider, and M. Siegel. *Finite Mathematics & Its Applications.* 10th ed. Pearson/Prentice Hall. (2010).

[5] M. Lial, R. Greenwell, and N. Ritchey. *Finite Mathematics and Calculus with Applications*. 10th ed. Pearson/Prentice Hall. (2011).

[6] W. Stein, et al, Sage Mathematics Software. The Sage Development Team, 2015.

`http://www.sagemath.org/`

[7] S. Tan. *Finite Mathematics for the Managerial, Life, and Social Sciences.* 7th ed. Thomson Brooks/Cole. (2003).

GINI-Coefficient, GOZINTO-Graph and Option Prices

Josef Böhm, ACDCA & DERIVE User Group, nojo.boehm@pgv.at

Abstract: GINI-Coefficient together with LORENZ-curve and GOZINTO-Graphs are economic applications of secondary school mathematics. They are part of the curriculum in Austria's Colleges for Business Administration (= Handelsakademie). Basic knowledge about stocks and options became important during the last years. Treating these issues are easy using technology.

The GOZINTO-Graph or GOZINTO-Chart is a pictorial representation that shows how the elements required to build a product fit together. This is often the first step for several planning functions especially for material requirements planning, for time and manpower resources planning, for production cost, etc.

This chart gives the input for building the production matrix. Easy to understand, and supported by technology, easy to perform matrix calculations, lead to the results.

Students can easily be inspired to design own tasks. Examples of students' works will be presented.

The GINI-Coefficient is a means for measuring the income distribution – and other distributions - of a nation's population. It is commonly used as a measure of inequality of income or wealth.

This sounds a little bit complicated but in fact it is an easy to perform application of integration based on the modelling of the so called LORENZ-Curve. We should be happy to find an application of definite integral which is not only calculation of the area between two curves.

Calculation of option prices is based on stock data (average rate of return, volatility, and other statistics – all well known in school). We will demonstrate the binomial model and the extend to the famous Black-Scholes formula.

When Mathematics Meet Computer Software

M. Beaudin, F. Henri

École de technologie supérieure (ÉTS), Montréal, Québec, Canada
michel.beaudin@etsmtl.ca, frederick.henri@etsmtl.ca

TI-Nspire CAS, from Texas Instruments, is the current computer algebra system used for both undergraduate level mathematics and science courses at ÉTS. While not as powerful as Maple or Mathematica, it offers some advantages over its competitors, mainly being multi-platform (calculator and computer) and easy to use. However, the lack of some useful functions becomes obvious when someone wants to perform higher mathematical development. A fruitful collaboration between the authors has produced interesting developments regarding the integration of piecewise functions [1] and the convolution of signals [2]. This talk will focus on our latest additions to the TI-Nspire system, namely automating the series solution for first and second order ODEs.

References

[1] Michel Beaudin, Frédérick Henri, Geneviève Savard. Integration of Piecewise Continuous Functions. The Derive Newsletter 91 (2013) 3–21. http://www.austromath.at/dug/dnl91.pdf

[2] Michel Beaudin. https://cours.etsmtl.ca/seg/mbeaudin/Liste_WEB.pdf

Revival of a Classical Topic in Differential Geometry: Envelopes of Parameterized Families of Curves and Surfaces

Th. Dana-Picard[1], N. Zehavi[2]

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

[2] *Weizmann Institute, nurit.zehavi@weizmann.ac.il*

Classical topics in Differential Geometry like the study of 1-parameter families of curves and surfaces in 3D space and their envelopes have been abandoned in the past for various reasons [4]. Nevertheless, this topic has a great interest in mathematics and in applied science. The topic has lots of applications in science and engineering - caustics and wave fronts, i.e. Geometrical Optics and Theory of Singularities, robotics and kinematics, rigid motion in 2-space and in 3-space, collision avoidance, etc. Envelopes can be studied with paper-and-pencil together with both a Computer Algebra System (CAS) and a Dynamical Geometry System (DGS); see recent papers in [5]. For this work, we used more than one package.

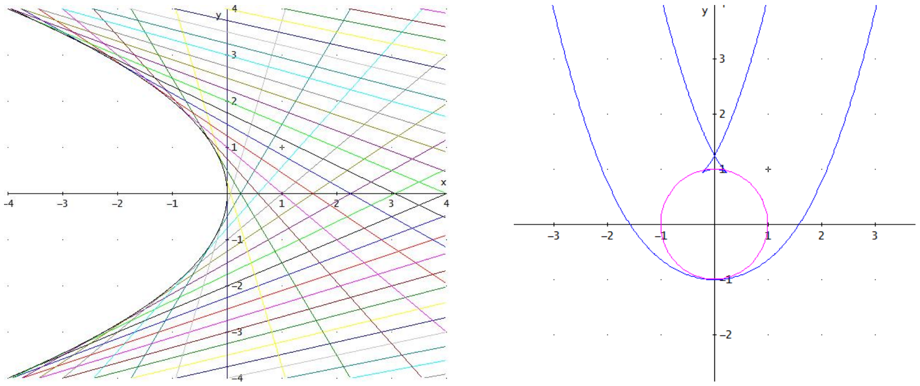
The authors performed similar work for another topic in classical Differential Geometry, namely isoptic curves of a given plane curve; see [1]. The influence of the technology was important. Here,as we will see, dynamical features are central.

Let be given a family of plane curves by an equation of the form $f(x,y,c)=0$, where c is a real parameter. An envelope of the family, if it exists, is a curve tangent to every curve in the family. It can be shown that this envelope is the solution set of the system of equations

$$\begin{cases} f(x,y,c) & = 0 \\ \frac{\partial f}{\partial c} f(x,y,c) & = 0 \end{cases} \tag{1}$$

Figure 1 shows the envelope of the family of lines given by the equation $x + cy = c^2$, where c is a real parameter (it is the parabola whose equation is $y = -x^2/4$. and the envelope of the family of circles with radius 1 and center on the parabola whose equation is $y = x^2$ (here the result has two components, each component is an envelope of the family of circles).

In both cases, the usage of a slider bar enables to build envelopes experimentally. The experimental study may enhance the understanding either of the possible non-existence or of the possible non-uniqueness of an envelope. An example is displayed in Figure 2 for the family of circles whose radius is equal to 1 and whose center runs on an ellipse. On the left a partial construction is shown, a global construction appears on the right. This drawing has been obtained using the slider bar,



(a) Lines

(b) Circles

Figure 1: Exploration of an envelope in the plane

which yields a uniform spacing between circles. Another possibility offered by the software is to move the center of the circle along the ellipse. In this case, spacing between neighboring circles is not uniform, the appearance of the envelopes being thus slightly different.

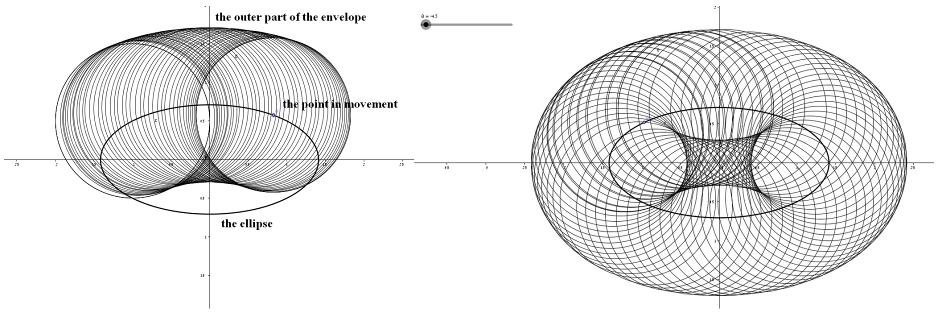


Figure 2: Dynamical exploration of the envelope of a family of circles

The transition to parameterized families of curves and surfaces in 3D space rely on the same techniques. For a 1-parameter family of surfaces, the defining equations for an envelope are now:

$$\begin{cases} f(x,y,z,c) & = 0 \\ \frac{\partial f}{\partial c} f(x,y,z,c) & = 0 \end{cases} \tag{2}$$

New issues have to be dealt with: the general visualization problems in this case, the availability of appropriate features in the software, etc. For the family of surfaces given by the equation $x + cy + c^2z = c^3$, where c is a real parameter, an envelope can be found, shown in Figure 3. A cuspidal edge appears, as for every 1-parameter family of planes. In order to understand the surface visually, dynamical features of the software are a must. Otherwise, at least two stills pictures have to been plotted. In particular in such a case, the structure of the envelope as a ruled surface can be studied using technology. This topic is sometimes not easy for beginning students. We could check the influence of the choice of the mesh for plotting surfaces in 3D space on the students' understanding. For example, in Figure 3, lines can be seen who are tangent to the cuspidal edge; this is a central feature of such an envelope.

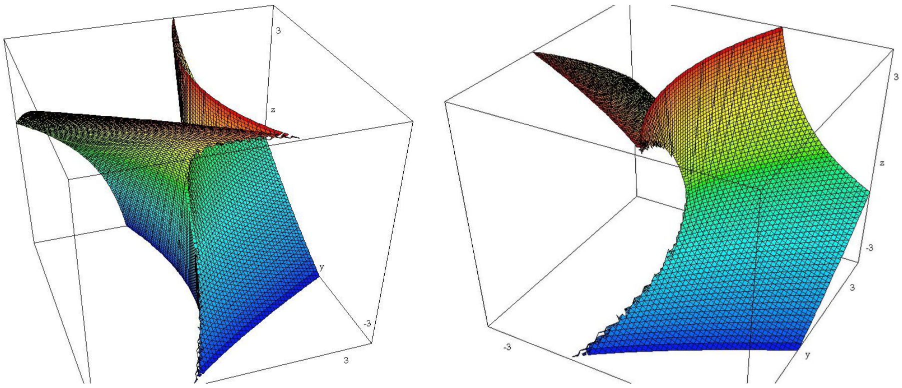


Figure 3: Exploration of the envelope of a family of planes

Such a study provides an opportunity to discover new topics beyond the scope of the regular curriculum, sometimes together with applications to practical situations. New computation skills with technology may be developed, in particular for the experimental aspect of the work (e.g., exploring the existence of cusps, as in Figure 1b). For this, the availability in the software of a slider bar is a central issue. Moreover, ability to switch between different registers of representation may be improved, within mathematics themselves (parametric vs implicit) and with the computer (algebraic, graphical, etc.).

An envelope may not exist (e.g. for a family of lines where the coefficients of the equations are affine functions of the parameter). These issues have been observed by the authors in sessions for in-service teachers at the Weizmann Institute of Science.

The algebraic engine we used in different CAS was the commands based on computations of Gröbner bases in order 1) to solve the given system of equations, which yields a parametric representation of the envelopes, and 2) to look for an implicitization of this parametric representation. The Gröbner bases algorithms have been widely used by Pech [2] for other geometric problems. When such an implicitization is not to be found, algorithms exist for an approximate implicitization (see [3]).

References

[1] Dana-Picard, Th., Mann, G. and Zehavi, N. *Bisoptic curves of a hyperbola*, International Journal of Mathematical Education in Science and Technology **45 (5)**, pp. 762-781 (2014).

[2] Pech, P. *Selected Topics In Geometry With Classical Vs. Computer Proving*, World Scientific (2007).

[3] Pottman, H. and Peternell, M. *Envelopes Computational Theory and Applications*, in *Proceedings of Spring Conference in Computer Graphic*, Budmerice, Slovakia, pp. 3-23 (2000).

[4] Thom, R. *Sur la théorie des enveloppes*. Journal de Mathématiques Pures et Appliquées, XLI (2), pp. 177-192 (1962).

[5] DNL 97. Derive Newsletter 97, April 2015. Available: http://www.austromath.at/dug/dnl97.pdf

Generating animations of JPEG images of closed surfaces in space using Maple and Quicktime

G. Labelle[1]

[1] *Université du Québec à Montréal (UQAM), Canada, labelle.gilbert@uqam.ca*

Too often, in undergraduate several variables calculus courses, surfaces are presented essentially only in the form,

$$z = f(x,y), \text{ or its variants, } y = g(x,z), x = h(y,z), \tag{1}$$

instead of the more symmetrical and versatile parametric form,

$$x = x(u,v), \quad y = y(u,v), \quad z = z(u,v). \tag{2}$$

Forms (1) are not very well adapted to evaluate surface integrals in order to illustrate, for example, the divergence theorem for closed surfaces in 3D space (such as a deformed sphere or twisted torus). Indeed, one must decompose the surface into smaller pieces and use several variants of (1) to compute double integrals which are then added or substracted taking into account various orientation issues.

In this talk, we show how to use periodic functions of u and v in the parametric form (2), to generate, via Maple, various large high quality JPEG images of closed surfaces in space for which the surface integrals are easily computed, among other things. Moreover, we also use QuickTime to pass from one surface to another in a very smooth animated way. Many examples as well as the Maple code used are given. Students are then able to easily generate their own surfaces and analyse their various geometrical properties in a very stimulating and colorful way.

References

[1] G. Labelle, *Des surfaces animées qui respirent dans l'espace*, Bulletin AMQ, vol. 50, no.4, 49-58 (2010). `http://archimede.mat.ulaval.ca/amq/Bulletins.html`

[2] G. Labelle, `http://www.lacim.uqam.ca/~gilbert`

Plotting technologies for the study of functions of two real variables

David Zeitoun[1] and Thierry Dana-Picard[2]

[1] *Department of Mathematics, Orot College of Education, Rehovot, Israel, ed.technologie@gmail.com*
[2] *Department of Mathematics, Jerusalem College of Technology, Jerusalem , Israel, ndp@jct.ac.il*

Students learning towards a degree in a STEM related domain learn quite early a course in Advanced Calculus, i.e. a course where the main object of study are multivariable functions. It happens that students cannot *see* how these objects behave. In particular, difficulties appear in classroom for functions having different limits at a point, according to the path approaching the point. Therefore dynamical visualization techniques are important.

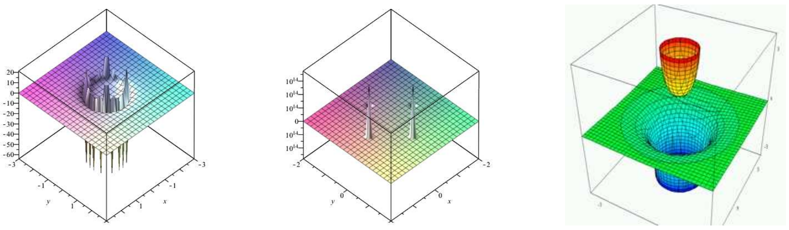
The study of functions of two real variables can be supported by visualization using a Computer Algebra System (CAS). Contour plots were the first type of graphic representations. With the development of scientific computing, 3D plots were introduced and plotting the graph of a two-variable function has been made possible, including parametric plotting and implicit plotting.

Depending both on the hardware and on the software, constraints exist, making sometimes the plots non accurate. For example, the choice of the mesh (using a triangulation of the domain, or using geodesics on the surface, etc.) has a great influence on the representation. Interpolations are performed, which may hide discontinuities. Other constraints come from the need to control the geometric transformations of the plotted surface: transformations such as zooming, rotation around a given axis, displacement along a given path are examples where the visualization device needs to understand the mathematical behavior of the function.

Here are examples of non-accurate plots, obtained with a brute force usage of commands, without a suitable analysis of the function. The function we tried to plot in Figure 1 is given by $f(x,y) = \frac{1}{1-(x^2+y^2)}$. The only difference in the command that has been entered is the x-intervals and the y-intervals, $[-2,2]$ in (a) and $[-3,3]$ in (b). The rightmost plot is quite accurate, it uses other techniques.

In the unaccurate plots, interpolations hide the actual discontinuities in different ways. Regular zooming cannot solve this problem, as it inflates the cells but does not recompute the needed numerical data.

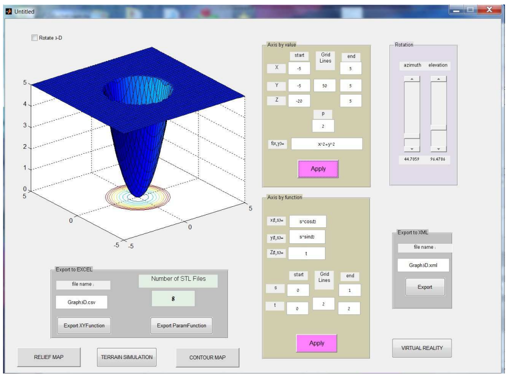
Rotation around a given axis often masks discontinuities of the function and can also provide strange plots, not compatible with the mathematics. In recent years, point based geometry has gained increasing attention as an alternative surface representation, both for efficient rendering and for flexible geometry process-



(a) (b) (c)

Figure 1: Strange plots

ing of complex surfaces. More sophisticated representations that use lighting effects and virtual reality are available. We analyze the efficiency of the different representations with respect to the mathematical behavior of a function of two real variables.



☐ Rotate 3-D

	start	Grid Lines	end
X	-5		5
Y	-5	50	5
Z	-20		5

p: 2

f(x,y)= x^2+y^2

azimuth: 44.7059 elevation: 96.4706

x(t,s)= s*cos(t)

y(t,s)= s*sin(t)

Z(t,s)= t

	start	Grid Lines	end
s	0		1
t	0	2	2

file name : Graph3D.csv

Number of STL Files: 8

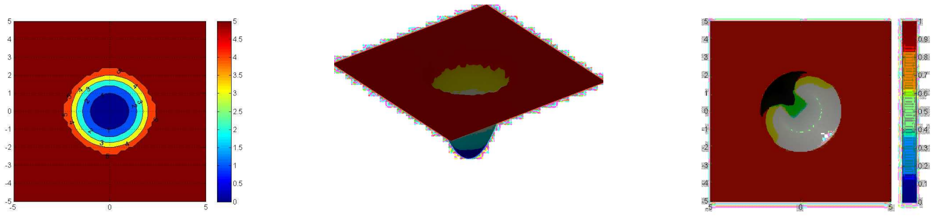
file name : Graph3D.xml

Figure 2: Interface

An interface written in Matlab 14 has been developed for producing different representations of a given explicit function of two variables; (see Figure 2). After having received an analytic expression for the function, the software produces four types of representation, namely:

1. A color contour map of the function.
2. A three dimensional plot of function.
3. A relief terrain map corresponding to the height of the function.
4. A virtual reality scene where the function is a terrain and the user is flying over it.

The first three representations are illustrated for the function given by $f(x,y) = x^2 + y^2$ in Figure 3. Note that this function has a discontinuity at $(0,0)$.



(a) Contours

(b) 3D plot

(c) Terrain relief

Figure 3: Color plottings

The virtual reality scene is shown for the same function in Figures (4 and 5).

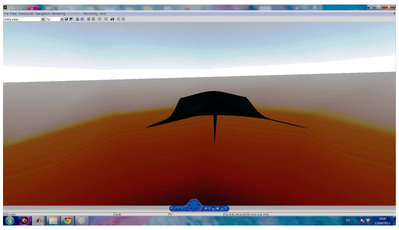


Figure 4: Virtual scene

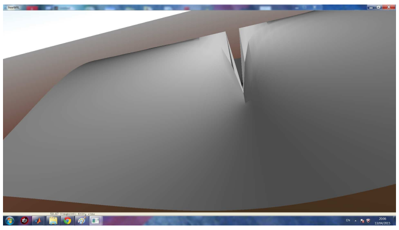


Figure 5: Path along a discontinuity

Comparison between the different kinds of representation is done with respect to the accuracy and the teaching of:

1. The global plotting of the function.
2. The appearance of the existing discontinuities and the non-appearance of non-existing discontinuities.

3. The visualization of directional derivatives.
4. The different types of optima, such as maximum. minimum points and saddle points.

Some of the issues that are to be discussed are as follows, all of them have an influence on the joint work of the students and the educator :

- The domain of the given function may be unbounded. Nevertheless, the plotting domain is always bounded; this is one of the constraints mentioned previously.
- Meshing techniques versus isoclines plotting.

This comparison and its outcome were an incitement to the usage of virtual reality in order to represent a function of two variables. In particular, the VR device under development is designed to generate paths on the surface under study and to replace classical zooming which only inflates the existing cells of the mesh by a re-computation of the data required for the plotting. This may allow to visualize clearly discontinuities and different types of extrema.

References

[1] Amenta N, Bern M, Kamvysselis M. *A new Voronoi - based surface reconstruction algorithm*. In: Proceedings of ACM SIGGRAPH 98, pp. 415-21 (1998).

[2] Botsch M, Kobbelt L., *Resampling feature and blend regions in polygonal meshes for surface antiÂaliasing. In: Proceedings of Eurographics* 01, pp. 402-10 (2010).

[3] Th. Dana-Picard: *Enhancing conceptual insight: plane curves in a computerized learning environment*, International Journal of Technology in Mathematics Education **12** (1), pp. 33-43, (2005).

[4] Th. Dana-Picard, I. Kidron and D. Zeitoun: *To See or not To See II*, International Journal of Technology in Mathematics Education 15 (4), pp. 157-166, (2008).

[5] Dos Santos S.R. and Brodlie K.W., *Visualizing and Investigating Multidimensional Functions*, IEEE TCVG Symposium on Visualization, pp. 1-10. Joint EUROGRAPHICS, (2002).

[6] Kobbelt L. and Botsh M., *A survey of point-based techniques in computer graphics*, Computer and Graphics **28**, pp. 801-814, (2004).

[7] Kobbelt L, Botsch M, Schwanecke U, Seidel HÂP. *Feature sensitive surface extraction from volume data*, in *Proceedings of ACM SIGGRAPH* 01, pp. 57-66, (2001).

[8] Dana-Picard Th. , Badihi Y. , Zeitoun D. and Israeli O., *Dynamical Exploration of Two-Variable Functions Using Virtual Reality*, Proceedings of CERME 6, Lyon (France), (2009).

[9] Zeitoun D.G. and T. Dana Picard *Accurate visualization of graphs of functions of two real variables*, International Journal of Computational and Mathematical sciences Vol 4 (1), pp. 1-11, (2010).

[10] Zeitoun D.G., Laible J.P. and G.F. Pinder, *An Iterative Penalty Method for the Least Squares Solution of Boundary Value Problems*, Numer. Meth. for P.D.E. **13**, pp. 257-281, (1997).

Some remarks on Taylor's polynomials visualization using Mathematica in context of function approximation.

Włodzimierz Wojas[1], Jan Krupa[2]

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

In this paper the authors critically analyse popular way of graphic presentation Taylor's polynomials in context of function approximation. They discuss the difficulties of presentation the best local polynomial approximation of function by Taylor's polynomials. Proposed by the authors method of graphical presentation based on table of function and Taylor's polynomials values in neighbourhood of a chosen point. For graphical presentation ListPlot and Plot functions with logarithmic scale in Mathematica System is used.

Introduction

Taylor's theorem is one of the most classic results of university course in calculus or mathematical analysis. For the case of one variable function $y = f(x)$ and point $x = x_0$, Taylor's polynomial of the n-th order is defined as:

$$T_n(x) = f(x_0) + \frac{f'(x_0)}{1!}(x - x_0) + \frac{f''(x_0)}{2!}(x - x_0)^2 + \cdots + \frac{f^{(n)}(x_0)}{n!}(x - x_0)^n$$

where a function $f(x)$ have at a point x_0 finite derivatives up to the n-th order inclusively. Many academic books e.g. [1, 2, 3, 4] contain graphs presented Taylor's polynomials for some elementary functions. For example for $f(x) = e^x$ or $f(x) = \sin x$ as is shown in Figures 1,2. Often these graphs are presented with comments that it shows how well these polynomials approximate $y = f(x)$ near a point $x = x_0$ when n increases.

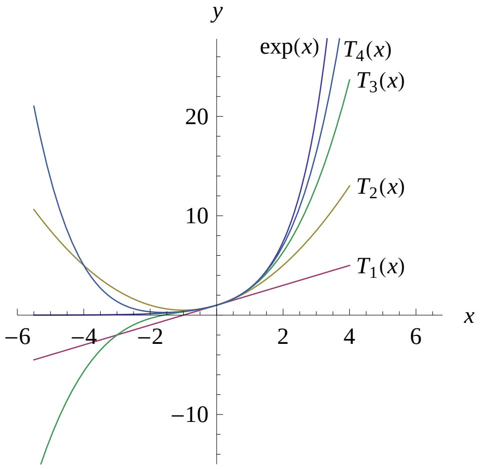


Figure 1: Taylor's polynomials $T_1(x)$, $T_2(x)$, $T_3(x)$, $T_4(x)$ for function $f(x) = e^x$ at point $x_0 = 0$.

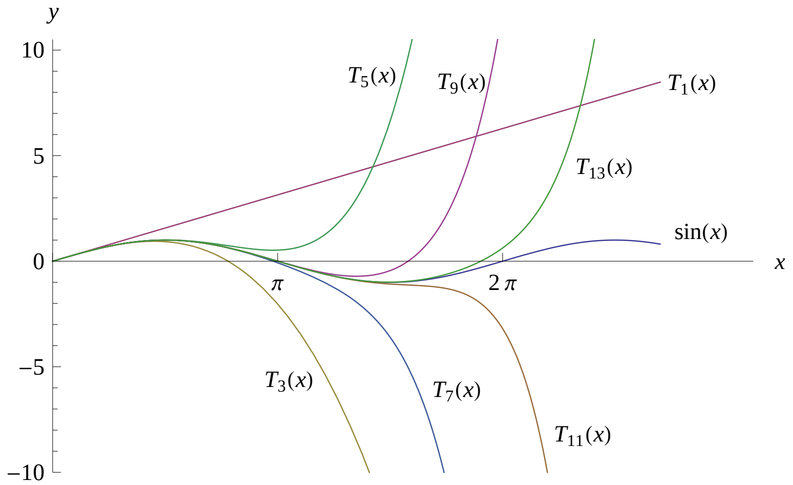


Figure 2: Taylor's polynomials $T_1(x)$, $T_3(x), \ldots, T_{13}(x)$ for function $f(x) = \sin x$ at point $x_0 = 0$.

1 Visualization of Taylor's polynomials in context of function approximation

Visualization of Taylor's polynomials is easy and comfortable using CAS packages such as Mathematica, Maple, Derive or others. For a one variable function Mathematica package contains standard procedure Series$[f,\{x,x0,n\}]$ which generates Taylor's polynomial of the n-th order for the function $f(x)$ and point $x = x_0$. Using procedure Plot$[\{f_1, f_2, \ldots, f_k\}, \{x, x_{min}, x_{max}\}]$ we can present graphs function $f(x)$ and some its Taylor's polynomials as is shown in Figures 1, 2. But this kind of presentation can be misleading for students in context of the function $f(x)$ approximation by Taylor's polynomials if we do not emphasize the fact of local character of this approximation. In Figures 3, 4 we see that graph of the function $f(x)$ and graphs of Taylor's polynomials seem to overlap close point $x = x_0$. On the base of these Figures we cannot settle which Taylor's polynomial better approximates the function close to the point x_0.

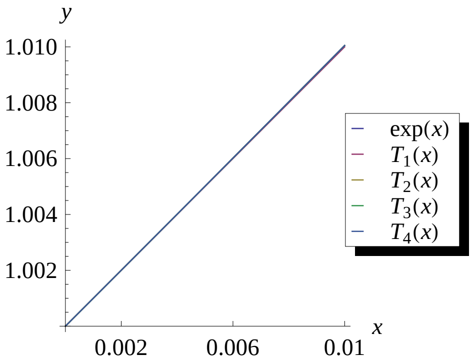


Figure 3: function $f(x) = e^x$ and its Taylor's polynomials $T_1(x)$, $T_2(x)$, $T_3(x)$, $T_4(x)$ in the reduced right neighbourhood $(0, 0.01)$ of the point $x_0 = 0$.

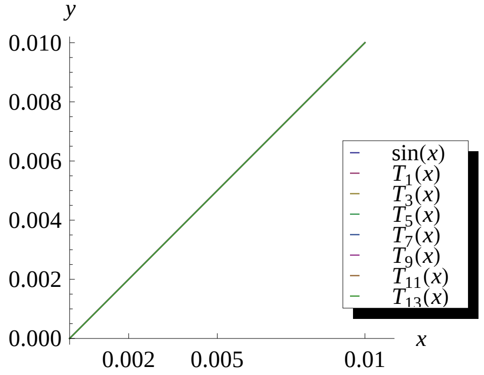


Figure 4: function $f(x) = \sin x$ and its Taylor's polynomials $T_1(x)$, $T_3(x), \ldots, T_{13}(x)$ in the reduced right neighbourhood $(0, 0.01)$ of the point $x_0 = 0$.

In Figures 1, 2 we see that graph of the function $f(x)$ and graphs of Taylor's polynomials seem to overlap close the point $x_0 = 0$. Next, Taylor's polynomials separate from the graph of the $f(x)$. Closer to the point x_0 separates Taylor's polynomial of lower order, further from the point x_0 separates Taylor's polynomial of higher order. Figures 1, 2 may suggest that overall Taylor's polynomial of higher order better approximates the function than Taylor's polynomial of lower order. But for example, for the function $f(x) = e^x$, $x_0 = 0$ and the point $x = -4$ it is easy to check that:
$T_2(x) = 1 + x + \dfrac{1}{2!}x^2, T_3(x) = 1 + x + \dfrac{1}{2!}x^2 + \dfrac{1}{3!}x^3$, $|f(-4) - T_2(-4)| = |e^{-4} - 5| < |f(-4) - T_3(-4)| = |e^{-4} + 17/3|$. So, $T_2(x)$ better approximates the function $f(x) = e^x$ at the point $x = -4$ than $T_3(x)$. Similarly, for the function $f(x) = \sin x$, $x_0 = 0$ and the point $x = \frac{5}{4}\pi$ we have:
$T_3(x) = x - \frac{1}{3!}x^3, T_5(x) = x - \frac{1}{3!}x^3 + \frac{1}{5!}x^5$, and $|f(\frac{5}{4}\pi) - T_3(\frac{5}{4}\pi)| \approx 5.46 < |f(\frac{5}{4}\pi) - T_5(\frac{5}{4}\pi)| \approx 7.88$. So, $T_3(x)$ better approximates the function $f(x) = \sin x$ at the point $x = \frac{5}{4}\pi$ than $T_5(x)$. Generally, Taylor's polynomial of higher order better approximates the function than Taylor's polynomial of lower order only locally in some neighbourhood of the point x_0.

2 Theorem of the best local polynomial approximation

This theorem and corollaries from it are inspired by theorem of the best local approximation presented in [5].

Let $P(x) = p_0 + p_1(x - x_0) + p_2(x - x_0)^2 + \ldots + p_m(x - x_0)^m$ and $Q(x) = q_0 +$

$q_1(x-x_0)+q_2(x-x_0)^2+\ldots+q_k(x-x_0)^k$ are different polynomials. Let r be the smallest nonnegative integer among numbers $i=0,1,2,\ldots$ which satisfy $p_i \neq q_i$ (if $m>k$ then we put $q_{k+1}=\ldots=q_m=0$, if $m<k$ then we put $p_{m+1}=\ldots=p_k=0$).

Assume that function $f(x)$ has finite derivative of n order at point x_0 and assume $r \leq n$.

Theorem. *If $p_i=\frac{f^{(i)}(x_0)}{i!}$ for all $i<r$ and $|\frac{f^{(r)}(x_0)}{r!}-p_r|<|\frac{f^{(r)}(x_0)}{r!}-q_r|$ then there exists such neighbourhood S of point x_0 such that $\bigwedge\limits_{x\in S}|f(x)-P(x)|<|f(x)-Q(x)|$.*

Proof. By Taylor's theorem we have: $f(x)-T_n(x)=(x-x_0)^n\omega(x)$, where $\omega(x)$ is a function continuous at x_0 and $\omega(x_0)=0$. Thus:

$$\begin{aligned}&|f(x)-P(x)|\\&=\Big|\left(\frac{f^r(x_0)}{r!}-p_r\right)(x-x_0)^r+\frac{f^{r+1}(x_0)}{(r+1)!}(x-x_0)^{r+1}+\cdots+\frac{f^n(x_0)}{n!}(x-x_0)^n\\&\qquad+(x-x_0)^n\omega(x)-p_{r+1}(x-x_0)^{r+1}-\cdots-p_m(x-x_0)^m\Big|,\end{aligned}$$

$$\begin{aligned}&|f(x)-Q(x)|\\&=\Big|\left(\frac{f^r(x_0)}{r!}-q_r\right)(x-x_0)^r+\frac{f^{r+1}(x_0)}{(r+1)!}(x-x_0)^{r+1}+\cdots+\frac{f^n(x_0)}{n!}(x-x_0)^n\\&\qquad+(x-x_0)^n\omega(x)-q_{r+1}(x-x_0)^{r+1}-\cdots-q_k(x-x_0)^k\Big|.\end{aligned}$$

Taking the factor $(x-x_0)^r$ out we have:

$$\begin{aligned}&|f(x)-P(x)|\\&=|(x-x_0)^r|\cdot\Big|\left(\frac{f^r(x_0)}{r!}-p_r\right)+\frac{f^{r+1}(x_0)}{(r+1)!}(x-x_0)+\cdots+\frac{f^n(x_0)}{n!}(x-x_0)^{n-r}\\&\qquad+(x-x_0)^{n-r}\omega(x)-p_{r+1}(x-x_0)-\cdots-p_m(x-x_0)^{m-r}\Big|.\end{aligned}$$

$$\begin{aligned}&|f(x)-Q(x)|\\&=|(x-x_0)^r|\cdot\Big|\left(\frac{f^r(x_0)}{r!}-q_r\right)+\frac{f^{r+1}(x_0)}{(r+1)!}(x-x_0)+\cdots+\frac{f^n(x_0)}{n!}(x-x_0)^{n-r}\\&\qquad+(x-x_0)^{n-r}\omega(x)-q_{r+1}(x-x_0)-\cdots-q_k(x-x_0)^{k-r}\Big|.\end{aligned}$$

The above equalities are true if $m > r$ and $k > r$. If $m \leq r$, then defining $p_{m+1} = p_{m+2} = \ldots = 0$ we have:

$$
\begin{aligned}
&|f(x) - P(x)| \\
&\quad = \Big| \left(\frac{f^r(x_0)}{r!} - p_r \right)(x - x_0)^r + \frac{f^{r+1}(x_0)}{(r+1)!}(x - x_0)^{r+1} + \cdots + \frac{f^n(x_0)}{n!}(x - x_0)^n \\
&\qquad\qquad + (x - x_0)^n \omega(x) \Big| \\
&\quad = |(x - x_0)^r| \cdot \Big| \left(\frac{f^r(x_0)}{r!} - p_r \right) + \frac{f^{r+1}(x_0)}{(r+1)!}(x - x_0) + \cdots + \frac{f^n(x_0)}{n!}(x - x_0)^{n-r} \\
&\qquad\qquad + (x - x_0)^{n-r} \omega(x) \Big|
\end{aligned}
$$

and if $k \leq r$ then defining $q_{k+1} = q_{k+2} = \ldots = 0$ we have:

$$
\begin{aligned}
&|f(x) - Q(x)| \\
&\quad = \Big| \left(\frac{f^r(x_0)}{r!} - q_r \right)(x - x_0)^r + \frac{f^{r+1}(x_0)}{(r+1)!}(x - x_0)^{r+1} + \cdots + \frac{f^n(x_0)}{n!}(x - x_0)^n \\
&\qquad\qquad + (x - x_0)^n \omega(x) \Big| \\
&\quad = |(x - x_0)^r| \cdot \Big| \left(\frac{f^r(x_0)}{r!} - q_r \right) + \frac{f^{r+1}(x_0)}{(r+1)!}(x - x_0) + \cdots + \frac{f^n(x_0)}{n!}(x - x_0)^{n-r} \\
&\qquad\qquad + (x - x_0)^{n-r} \omega(x) \Big|
\end{aligned}
$$

(both numbers k and m cannot be at the same time less than r).
As x approaches to x_0 we obtain:

$$
\begin{aligned}
&\lim_{x \to x_0} \Big| \Big(\frac{f^r(x_0)}{r!} - p_r \Big) + \frac{f^{r+1}(x_0)}{(r+1)!}(x - x_0) + \cdots + \frac{f^n(x_0)}{n!}(x - x_0)^{n-r} \\
&\qquad + (x - x_0)^{n-r} \omega(x) - p_{r+1}(x - x_0) - \cdots - p_m(x - x_0)^{m-r} \Big| \\
&\qquad\qquad = \Big| \frac{f^r(x_0)}{r!} - p_r \Big|,
\end{aligned}
$$

$$
\begin{aligned}
&\lim_{x \to x_0} \Big| \Big(\frac{f^r(x_0)}{r!} - q_r \Big) + \frac{f^{r+1}(x_0)}{(r+1)!}(x - x_0) + \cdots + \frac{f^n(x_0)}{n!}(x - x_0)^{n-r} \\
&\qquad + (x - x_0)^{n-r} \omega(x) - q_{r+1}(x - x_0) - \cdots - q_k(x - x_0)^{k-r} \Big| \\
&\qquad\qquad = \Big| \frac{f^r(x_0)}{r!} - q_r \Big|.
\end{aligned}
$$

Because of our assumption $\left|\frac{f^{(r)}(x_0)}{r!} - p_r\right| < \left|\frac{f^{(r)}(x_0)}{r!} - q_r\right|$ and the last two limits we conclude that there exists such neighbourhood S of point x_0 such that

$$\begin{aligned}\bigwedge_{x\in S}\Big|\Big(\frac{f^r(x_0)}{r!} - p_r\Big) + \frac{f^{r+1}(x_0)}{(r+1)!}(x-x_0) + \cdots + \frac{f^n(x_0)}{n!}(x-x_0)^{n-r} \\ + (x-x_0)^{n-r}\omega(x) - p_{r+1}(x-x_0) - \cdots - p_m(x-x_0)^{m-r}\Big| \\ < \Big|\Big(\frac{f^r(x_0)}{r!} - q_r\Big) + \frac{f^{r+1}(x_0)}{(r+1)!}(x-x_0) + \cdots + \frac{f^n(x_0)}{n!}(x-x_0)^{n-r} \\ + (x-x_0)^{n-r}\omega(x) - q_{r+1}(x-x_0) - \cdots - q_k(x-x_0)^{k-r}\Big|\end{aligned}$$

Multiplying both sides of the last inequality by $|(x-x_0)^r|$ we obtain that $\bigwedge_{x\in S} |f(x) - P(x)| < |f(x) - Q(x)|$.
In cases $m \le r$ or $k \le r$ the proof is analogous. □

Corollary 1. *Let $Q(x)$ be a polynomial which satisfies: there exists i ($i \le n$) such that $q_i \neq \dfrac{f^{(i)}(x_0)}{i!}$ (if $m < n$ then we define $q_{m+1} = q_{m+2} = \ldots = q_n = 0$). Then there exists such neighbourhood S of point x_0 such that, $\bigwedge_{x\in S} |f(x) - T_n(x)| < |f(x) - Q(x)|$. Particularly $Q(x)$ can be any polynomial of order not greater than n different than $T_n(x)$.*

Corollary 2. *There exists such neighbourhood S of point x_0 such that,*
$\bigwedge_{x\in S} |f(x) - T_n(x)| \le |f(x) - T_{n-1}(x)| \le \ldots \le |f(x) - T_1(x)|$,
where every inequality from the last sequence of inequalities becomes equality if and only if when the two consecutive Taylor's polynomial of $f(x)$ in both sides of the inequality are identical.

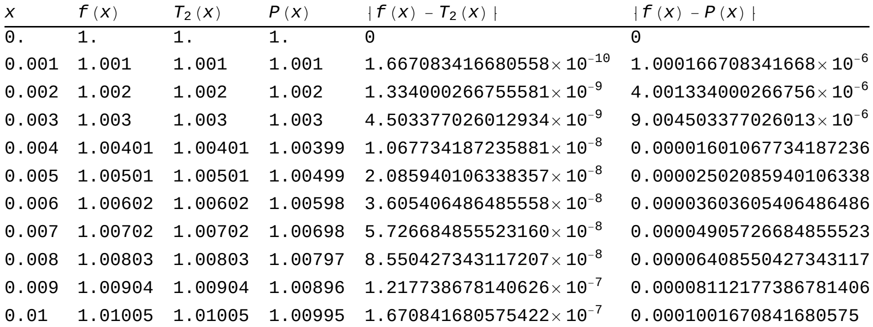
3 Visualization of the best locally approximation by Taylor's polynomials with Mathematica

Let us visualize Corollary 1 and 2 for reduced right neighbourhood $(0, 0.01)$ of the point $x_0 = 0$ using Wolfram Mathematica System [6, 7].

Example 1. For the Corollary 1 we define: $f(x) = e^x$, $x_0 = 0$, $T_2(x) = 1 + x + \frac{1}{2!}x^2$ and $P(x) = 1 + x - \frac{1}{2!}x^2$ for $x \in (0, 0.01)$. By Taylor's theorem we get:
$e^x - T_2(x) = e^x - (1 + x + \dfrac{1}{2!}x^2) = \dfrac{1}{3!}(e^{\tilde{x}})x^3 > 0$

and $e^x - P(x) = 1 + x + \frac{1}{2!}x^2 + \frac{1}{3!}(e^{\tilde{x}})x^3 - (1 + x - \frac{1}{2}x^2) = x^2 + \frac{1}{3!}(e^{\tilde{x}})x^3 > 0$ for $\tilde{x} \in (0,x), x \in (0,0.01)$.
Hence, we have: $|f(x) - T_2(x)| - |f(x) - P(x)| = e^x - (1 + x + \frac{1}{2}x^2) - e^x + 1 + x - \frac{1}{2}x^2 = -x^2 < 0$
and finally $\bigwedge\limits_{x \in (0,0.001)} |f(x) - T_2(x)| < |f(x) - P(x)|$.

Let us visualize this inequality by creating a table of numerical values for both sides of inequality with step 0.001.



x	$f(x)$	$T_2(x)$	$P(x)$	$\mid f(x) - T_2(x)\mid$	$\mid f(x) - P(x)\mid$
0.	1.	1.	1.	0	0
0.001	1.001	1.001	1.001	$1.667083416680558 \times 10^{-10}$	$1.000166708341668 \times 10^{-6}$
0.002	1.002	1.002	1.002	$1.334000266755581 \times 10^{-9}$	$4.001334000266756 \times 10^{-6}$
0.003	1.003	1.003	1.003	$4.503377026012934 \times 10^{-9}$	$9.004503377026013 \times 10^{-6}$
0.004	1.00401	1.00401	1.00399	$1.067734187235881 \times 10^{-8}$	0.00001601067734187236
0.005	1.00501	1.00501	1.00499	$2.085940106338357 \times 10^{-8}$	0.00002502085940106338
0.006	1.00602	1.00602	1.00598	$3.605406486485558 \times 10^{-8}$	0.00003603605406486486
0.007	1.00702	1.00702	1.00698	$5.726684855523160 \times 10^{-8}$	0.00004905726684855523
0.008	1.00803	1.00803	1.00797	$8.550427343117207 \times 10^{-8}$	0.00006408550427343117
0.009	1.00904	1.00904	1.00896	$1.217738678140626 \times 10^{-7}$	0.00008112177386781406
0.01	1.01005	1.01005	1.00995	$1.670841680575422 \times 10^{-7}$	0.0001001670841680575

Table 1: the values of $f(x)$, $T_2(x), P(x)$, $|f(x) - T_2(x)|$ and $|f(x) - P(x)|$ with step 0.001

We see in Table 1 that for all considered points inequality is true. Based on the Table1 we can prepare Figure 5 using logarithmic scale. Increasing WorkingPrecision and Accuracy in Mathematica Plot function we can get the continous graphs presented in Figure 6

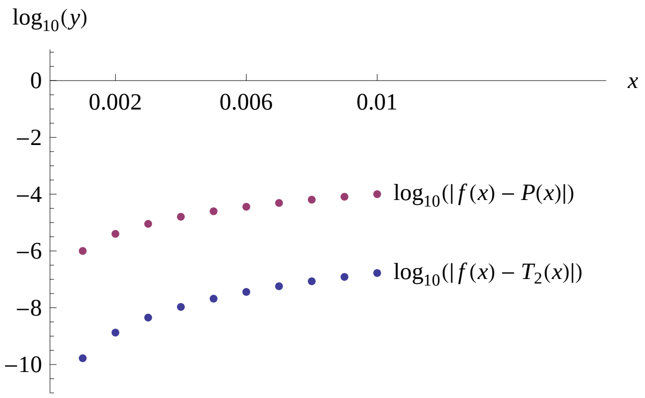


Figure 5: discrete graphs of $|f(x) - T_2(x)|$ and $|f(x) - P(x)|$ in reduced right neighbourhood $(0, 0.01)$ of the point $x_0 = 0$ with logarithmic scale using Mathematica Plot function.

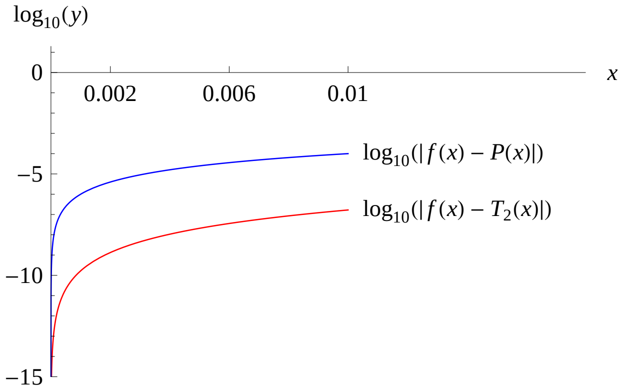


Figure 6: continuous graphs of $|f(x) - T_2(x)|$ and $|f(x) - P(x)|$ in reduced right neighbourhood $(0, 0.01)$ of the point $x_0 = 0$ with logarithmic scale using Mathematica Plot function.

In Figure 5 we see that the graphs of $|f(x) - T_2(x)|$ and $|f(x) - P(x)|$ are separated and that $|f(x) - T_2(x)| < |f(x) - P(x)|$ for $x \in (0, 0.01)$.

Example 2. For the Corollary 2 we define: $f(x) = \sin x, x_0 = 0$,
$T_3(x) = x - \frac{1}{3!}x^3$,
$T_7(x) = x - \frac{1}{3!}x^3 + \frac{1}{5!}x^5 - \frac{1}{7!}x^7$,

$T_{11}(x) = x - \frac{1}{3!}x^3 + \frac{1}{5!}x^5 - \frac{1}{7!}x^7 + \frac{1}{9!}x^9 - \frac{1}{11!}x^{11}$.
By Taylor's theorem, for all $x \in (0, 0.01)$ we have:
$f(x) - T_3(x) = (\frac{1}{4!}\sin\tilde{x})x^4 > 0$,
$f(x) - T_7(x) = (\frac{1}{8!}\sin\tilde{\tilde{x}})x^8 > 0$,
$f(x) - T_{11}(x) = (\dfrac{1}{12!}\sin\tilde{\tilde{\tilde{x}}})x^{12} > 0$,
where $\tilde{x}, \tilde{\tilde{x}}, \tilde{\tilde{\tilde{x}}} \in (0, x)$.
Hence, for all $x \in (0, 0.01)$ we get:

$$\begin{aligned}|f(x) - T_3(x)| - |f(x) - T_7(x)| &= f(x) - T_3(x) - f(x) + T_7(x) = \frac{1}{5!}x^5 - \frac{1}{7!}x^7 \\ &= \frac{1}{7!}x^5(42 - x^2) = \frac{1}{7!}x^5(\sqrt{42} - x)(\sqrt{42} + x) > 0,\end{aligned}$$

$$\begin{aligned}|f(x) - T_7(x)| - |f(x) - T_{11}(x)| &= f(x) - T_7(x) - f(x) + T_{11}(x) = \frac{1}{9!}x^9 - \frac{1}{11!}x^{11} \\ &= \frac{1}{11!}x^9(110 - x^2) = \frac{1}{11!}x^9(\sqrt{110} - x)(\sqrt{110} + x) > 0.\end{aligned}$$

So, finally $\bigwedge\limits_{x \in (0, 0.01)} |f(x) - T_3(x)| > |f(x) - T_7(x)| > |f(x) - T_{11}(x)|$.

Let us visualize this double inequality by create a table of values for all sides of inequality with step 0.001.

x	$f(x)$	$T_3(x)$	$T_7(x)$	$T_{11}(x)$	$\|f(x) - T_3(x)\|$	$\|f(x) - T_7(x)\|$	$\|f(x) - T_{11}(x)\|$
0.001	0.001	0.001	0.001	0.001	8.45678×10^{-18}	2.75573×10^{-33}	1.60590×10^{-49}
0.002	0.002	0.002	0.002	0.002	2.66714×10^{-16}	1.41093×10^{-30}	1.31556×10^{-45}
0.003	0.003	0.003	0.003	0.003	2.02529×10^{-15}	5.42411×10^{-29}	2.56033×10^{-43}
0.004	0.00399999	0.00399999	0.00399999	0.00399999	8.53397×10^{-15}	7.22398×10^{-28}	1.07770×10^{-41}
0.005	0.00499998	0.00499998	0.00499998	0.00499998	2.60417×10^{-14}	5.38229×10^{-27}	1.96033×10^{-40}
0.006	0.00599996	0.00599996	0.00599996	0.00599996	6.47997×10^{-14}	2.77714×10^{-26}	2.09742×10^{-39}
0.007	0.00699994	0.00699994	0.00699994	0.00699994	1.40058×10^{-13}	1.11204×10^{-25}	1.55594×10^{-38}
0.008	0.00799991	0.00799991	0.00799991	0.00799991	2.73066×10^{-13}	3.69868×10^{-25}	8.82855×10^{-38}
0.009	0.00899988	0.00899988	0.00899988	0.00899988	4.92073×10^{-13}	1.06763×10^{-24}	4.08199×10^{-37}
0.01	0.00999983	0.00999983	0.00999983	0.00999983	8.33332×10^{-13}	2.75573×10^{-24}	1.60590×10^{-36}

Table 2: the values of $f(x), T_3(x), T_7(x), T_{11}(x), |f(x) - T_3(x)|, |f(x) - T_7(x)|$ and $|f(x) - T_{11}(x)|$ with step 0.001

We see in Table 2 that for all considered points double inequality is true. Based on the Table 2 we can prepare Figure 7 using logarithmic scale.

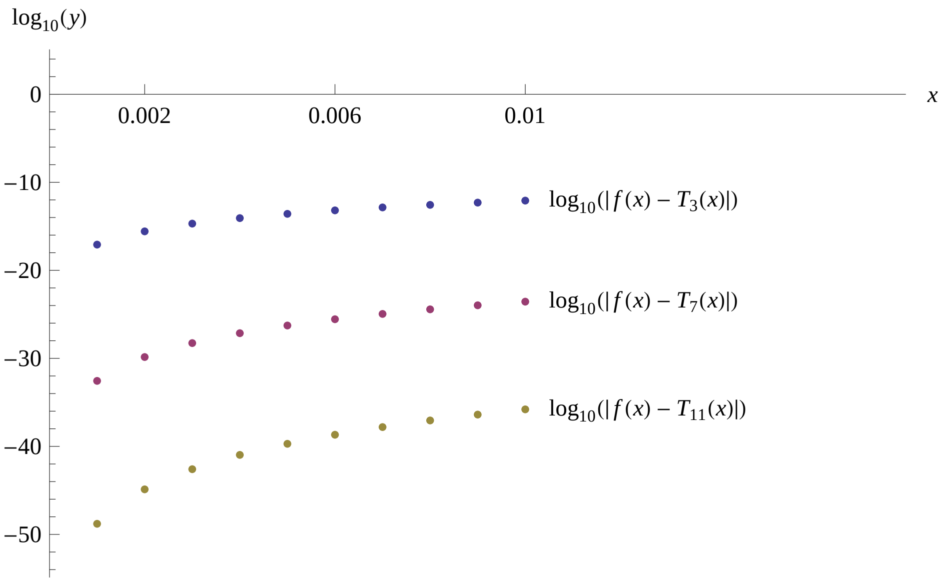


Figure 7: discrete graphs of $|f(x) - T_3(x)|, |f(x) - T_7(x)|$ and $|f(x) - T_{11}(x)|$ in reduced right neighbourhood $(0, 0.01)$ of the point $x_0 = 0$ with logarithmic scale using Mathematica ListPlot function.

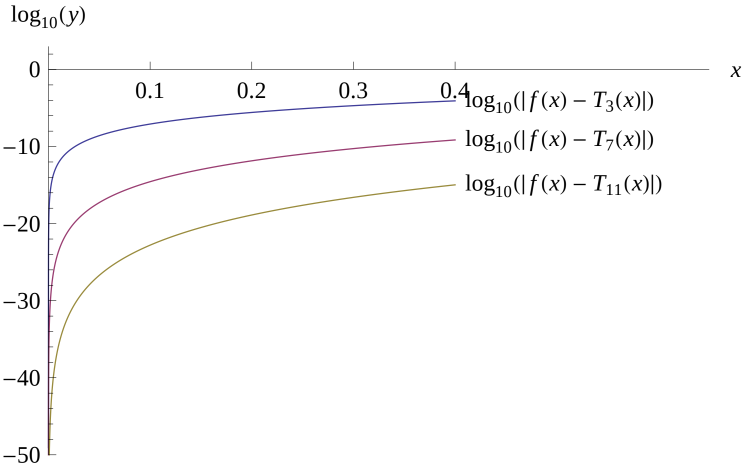


Figure 8: continous graphs of $|f(x)-T_3(x)|, |f(x)-T_7(x)|$ and $|f(x)-T_{11}(x)|$ in reduced right neighbourhood $(0,0.4)$ of the point $x_0 = 0$ with logarithmic scale using Mathematica Plot function.

In Figures 6 and 7 we see that graphs of $|f(x)-T_3(x)|, |f(x)-T_7(x)|$ and $|f(x)-T_{11}(x)|$ are separated.

Summary

In this paper the authors discuss graphic presentation of Taylor's polynomials in context of local approximation of a function. In popular way of graphic presentation Taylor's polynomials, graph of the function $f(x)$ and graphs of its Taylor's polynomials seem to overlap in a neighbourhood of the point $x = x_0$. Using logarithmic scale to present graphs we can separate graphs of differences between function and its Taylor's polynomials. To prepare graphs Mathematica System was used.

References

[1] G. B. Thomas, R. L. Finney, *Calculus and Analytic Geometry*, 9th ed., Addison-Wesley Publishing Company, 1998

[2] R. E. Larson, R.P. Hostetler, B. H. Edwards, *Calculus*, 6th ed., Houghton Mifflin Company, 1998

[3] C. H. Edwards, D. E. Penney, *Calculus*, Prentice Hall College Div, 1998

[4] G. N. Yakovlev, *Higher Mathematics*, Mir Publisher Moscow, 1990

[5] M.K. Grebencia, C. I. Novosielov, *A course of Mathematical Analysis*, Part 1 (in Russian), Moscow 1951

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

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

VISUALIZATION OF ORTHONORMAL TRIADS IN CYLINDRICAL AND SPHERICAL COORDINATES.

Jeanett López García*, Jorge J. Jiménez Zamudio*, Ma. Eugenia Canut Díaz Velarde*.
**FES Acatlán. UNAM, Mexico, jeanettlg@hotmail.com*

According with Committee on Programs for Advanced Study of Mathematics and Science in American High Schools (2002, p. 197), "the primary goal of advanced study in any discipline should be for students to achieve a deep conceptual understanding of the discipline's content and unifying concepts. Well-designed programs help students develop skills of inquiry, analysis, and problem solving so that they become superior learners."

If it is undoubted that abstraction is one of the skills that teachers wish to improve in their students, our first question is: Must teachers take advantage of technological resources such as CAS or DGS as a help in their classes in undergraduates courses and what kind of course could be the best for proving it really happen?

If we had to decide which courses can be a goal to use any kind of technological help, we will choose Geometry. Hilbert, D., and Cohn-Vossen, S. (1990, Preface, p. iii) said that Geometry has had a tendency to magnify some conceptual theories which make extensive use of abstract reasoning and symbolic calculation in the sense of algebra, but "with the aid of visual imagination we can illuminate the manifold facts and problems of geometry".

One concept, whose importance is both theoretical and practical, corresponds to the coordinate transformation, in particular orthogonal coordinate systems. We can use trigonometric constructions to find the transformation equations, i.e., the algorithm for passing of a Cartesian system, of two or three dimension, to other coordinate system, such as: polar, cylindrical or spherical coordinates. But if we add the knowledge and some techniques from Linear Algebra, for example following the reasoning of the book by Arfken & Weber (2005), we can introduce new mathematical properties, but we will increase considerably the abstract reasoning and symbolic calculation.

So, a second question arises: how we can increase the mathematical level and at the same time help students to understand this knowledge? We know that visualization helps intuitive understanding. Both of them play a major role in geometry. Therefore we propose using CAS and DGS to show how a triad, of basis vectors, is continuously changing of direction, keeping the norm vector without change, and we can match this visualization with the reasoning from theories of linear algebra.

References

Arfken, G., & Weber, H. (2005). Mathematical Methods for Physicists. USA: Elsevier.

Committee on Programs for Advanced Study of Mathematics and Science in American High Schools. (2002). Learning and Understanding. Improving Advanced Study Of Mathematics And Science In U.S. High Schools. Gollub, J., Bertenthal, M., Labov, J. & Curtis, P. Editors. Washington, D.C.: National Academy Press.

Hilbert, D., and Cohn-Vossen, S. (1990). *Geometry and the imagination,* Translated into English by P. Nemenyi from Anschauliche Geometrie. New York: Chelsea.

Contemporary interpretation of a historical locus problem with an unexpected discovery

R. Hašek

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

This talk is aimed primarily as a report on experience in the use of computer algebra (CAS) and dynamic geometry (DGS) systems in the teaching of future mathematics teachers. Specifically it deals with the detailed analysis of a historical locus problem selected from the Latin book *Exercitationes Geometricae* by Ioannis Holfeld, published by the Jesuit College of St. Clement in Prague in 1773 [3]; namely problem number 35 from a total of 47 solved problems that are presented in this book.

First, the original solution to problem 35 will be introduced. Then, it will be resolved using current methods supported by the use of GeoGebra and wxMaxima software. The different approach to the locus problem compared to the original solution allows us to reveal a more complete solution to the problem, which includes the surprising curve of a pretzel shape (a similar but not identical curve was mentioned in [1], see also `http://mathworld.wolfram.com/KnotCurve.html`). Finally we will derive both the algebraic equation and the parametric equations of the curve. All with the support of the mentioned software, as we solve it with students of mathematics teaching in the course of algebra and geometry.

Assignments of the problems in the book, as well as their solutions, illustrate the method of solving geometric problems typical for mathematics of the 17th and 18th centuries. Most of the problems, despite their age, are still attractive and are worth resolving with the help of contemporary methods. More information about the exercises, methods of their solutions and about the author of the book can be found in [2] and [4]. A copy of the original Latin assignments of the presented problem can be found at `http://www.pf.jcu.cz/~hasek/Holfeld`.

Problem 35: *Given a circle with a diameter MP (see Fig. 1); construct a radius AB to this circle and a line segment BO perpendicular to MP so that $MO : AO = r : BC$ (r is the radius of the circle). Find the locus of point C. (Remark: Length of the segment BC is the fourth proportional of lengths MO, AO and r.)* ([3], p. 41, *Problema 35*).

I. H. begins his solution by labeling lengths of selected segments; $AD = x$, $DC = y$, $AB = r$, $OM = z$. Then, using the similarity of triangles accompanied by the right triangle altitude theorem (also known as ‘geometric mean theorem’), however, without mentioning the use of it, he derives the locus equation $y^2 = r^2 - 2rx$ (considering the configuration of the coordinate axes in Fig. 2), that corresponds

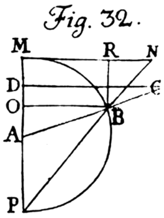


Figure 1: Illustration of the assignment of problem 35

to the parabola. Its plot for the particular value of r is shown in Fig. 2, left. On the right in the same figure the result is presented of the use of GeoGebra's tool "Locus" to find the desired locus curve. Considering all possible positions of point C on the ray AB with respect to point B we receive a surprising result. The curve consists of two parts; parabola, which was identified as the solution by I. H., and a curve that looks like a pretzel. To learn more about these curves we represent

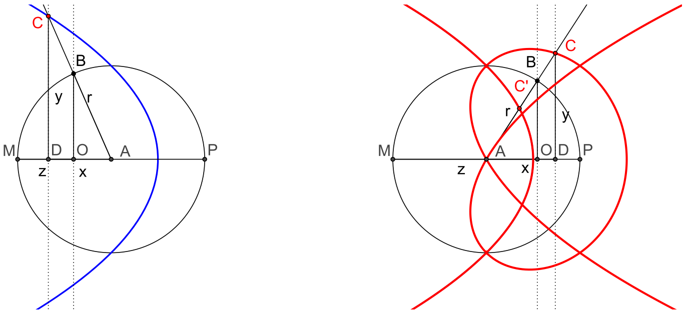


Figure 2: Solution of problem 35 according to I. H. (left) and the solution by means of GeoGebra's tool "Locus" (right)

the task by means of the system of nonlinear equations. Its solution by elimination leads to the sixth degree algebraic equation in the variables x and y, the polynomial of which can always be factored into the product of two polynomials of the second and fourth degree respectively (1).

$$(y^2+2rx-r^2)(y^4+x^2y^2-2rxy^2-2rx^3+3r^2x^2-r^2y^2)=0, \tag{1}$$

The second degree factor corresponds to the parabola (the solution given by I. H.) and the fourth degree factor defines the 'pretzel' curve, both curves shown in Fig. 2, right.

This unique event of the discovery of a new curve motivates us to explore its properties. Above all, we will focus on its parameterization. With the use of the computer we can introduce students to the principles of the parameterization of curves (see Fig. 3), illustrate it in examples and let them find the parametric equations of the new curve that are for example as follows

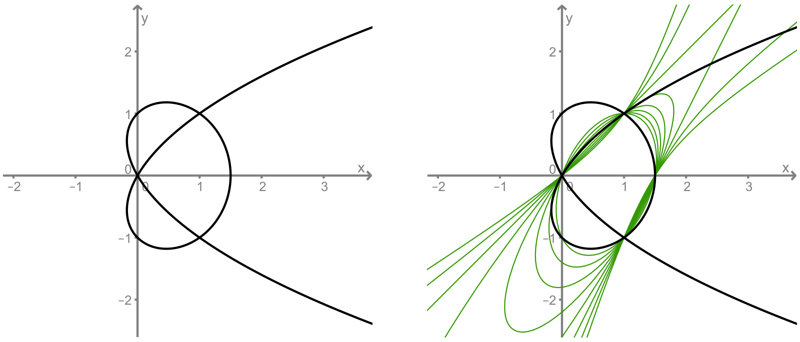


Figure 3: The discoveried curve and its parametrization by a system of conics

$$x = \frac{t^4 - 4t^2 + 3}{2t^2 + 2}, \quad y = \frac{t^3 - 3t}{t^2 + 1}. \tag{2}$$

We have experienced that the return to historical tasks can be inspiring and beneficial if the solver is equipped with analytical methods and the proper algebraic and dynamic geometry software. Through the study of the presented historical geometry problem, the solution of which has not been described in any textbook since the 18th century, students develop or practice their knowledge of the geometry of curves, polynomial algebra and the effective use of mathematical software.

References

[1] H.M. Cundy, *Mathematical models*, 2^{nd} ed., Oxford University Press, Oxford (1961).

[2] R. Hašek and J. Zahradník, *Study of historical geometric problems by means of CAS and DGS,* The International Journal for Technology in Mathematics Education, Research Information Ltd., Burnham, UK, Volume 22, Number 2 (it will be published in June) (2015).

[3] I. Holfeld, *Exercitationes Geometricae*, Charactere Collegii Clementini Societas Jesu, Praha (1773).

[4] J. Zahradník, *Problémy z geometrie ve sbírce Ioannise Holfelda Exercitationes geometricae* (in Czech), Sborník 34. mezinárodní konference Historie matematiky, Poděbrady, 23. - 27. srpna 2013, Matfyzpress, Praha, p. 191 (2013).

A Constructive Proof of Feuerbach's Theorem Using a Computer Algebra System

Michael Xue[1]

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

Feuerbach's Theorem states that the midpoints of the three sides, the base points of the three heights, and the midpoints of the line segments between the corners of a triangle and the intersection of the heights are on a circle. This talk offers a constructive proof. It is known that algebraic expression

$$x^2 + y^2 + dx + ey + f = 0 \tag{1}$$

represents a circle centered at $(-\frac{d}{2}, -\frac{e}{2})$ with radius

$$r^2 = \frac{d^2 + e^2 - 4f}{4} \tag{2}$$

provide (2) is positive. Three points among nine stated in the theorem are chosen to form a system of linear equations from (1). The values of *d, e* and *f* are determined by solving the equations. With the solution, (2) is shown to be positive which implies (1) indeed represents a circle. We then proceed to verify that the coordinates of the remain six points statisfy (1). Hence all nine points are on the same circle.

References

[1] B. Spain, *Analytical Conics* pp. 21-23 (2007).

[2] J. Gullberg, *Mathematics From the Birth of Numbers* p. 433 (1997).

Math Partner and Math Tutor

Gennadi Malaschonok and Natasha Malaschonok

Abstract. We consider the main features of the Web service Math Partner, as the training system (Math Tutor), which is designed to automate the work of the teacher

Currently, there are a lot of training systems both local, which are installed on users' computers, and «cloud», which are available in online mode. The main advantage of the system Math Partner in comparison with other learning systems is a multi-level feedback. It allows students to bring their solution of a problem to the correct result under the control of MathPartner.

Let us dwell on the description of the main features which allow to consider Web service Math Partner as a learning system that enables to automate the work of teachers.

1. A user if he is a student may register himself in the system MathPartner, but it is not necessary. The standard process of using the system supposes the registration by the administrator of educational institution.

2. Logging in with his password, the student will be able to use his curriculum, which must be loaded by his administrator or a teacher.

3. The solution of each task of the test must be put in the workbook of the student just after the task (online).

4. After finishing the solution of the test the student asks to check it. The system checks and informs the student about the rightness or wrongness of his answer. If the solution is wrong, the student returns and corrects it. He has the opportunity to look at the right solution if he can not solve the problem himself.

5. We organize two modes of problem solving: the student's independent work and tests. In the mode of control work a student can not know whether he solved the problem correct or not until he finishes all tasks.

6. The system calculates and stores the percentage of correctly solved problems of the test. It saves information about the number of attempts to solve each task.

7. In the mode of control work the student can keep all the solutions of problems in one file and send it to the teacher, if he doubts in the correctness of evaluations obtained from the system.

8. The system logs all events and keeps records available to all individuals who are interested in the successful completion of the educational process.

Let us dwell on the rules of recording solutions in the cloud workbook. The Language of the System is a dialect of TeX. Immediately after entering the system compiles the solutions resulting text into the PDF file, the solution of the problem is shown in the input field. The student can switch the form of notebook from the input language into the pdf-view and back by means of the system.

Conclusion

The system "MathPartner" as a mathematical web service exists during five years (for details see Ref. [1-4]). Now this service can be used for teaching math and other subjects in secondary schools and in higher education.

References

[1] http://MathPartner.com

[2] Malaschonok G.I. *Computer mathematics for computational network* // Tambov University Reports. Series Natural and Technical Sciences. Tambov, 2010. V. 15. Issue 1. P. 322-327. .

[3] Malaschonok G.I. *Language Guide "Mathpar"* .Tambov: Publishing House of TSU, 2013, 133pp.

[4] Malaschonok G.I. *Project of Parallel Computer Algebra* // Tambov University Reports. Series Natural and Technical Sciences. Tambov, 2010. V. 15. Issue 1. P. 1724-1729.

Gennadi Malaschonok
Institute of Mathematics, Physics and Informatics
Tambov State University
Tambov, Russia
e-mail: malaschonok@ya.ru

Natasha Malaschonok
Institute of Mathematics, Physics and Informatics
Tambov State University
Tambov, Russia
e-mail: namalaschonok@gmail.com

Ideas for Teaching Using CAS

M. BEAUDIN

École de technologie supérieure (ETS), Montréal (Québec), Canada, michel.beaudin@etsmtl.ca

Differential equations courses are among those where use of CAS is the most justified. Namely in engineering mathematics where heavy computations are difficult to perform by hand and many problems are dealing with applications. Unfortunately, the use of CAS is rarely applied to theoretical concepts students need to learn. In this talk, we will use TI-Nspire CAS technology and present differential equations examples where both applications and mathematical theory can be addressed together. Moreover, this approach will allow us to tackle some problems using two different methods, creating an opportunity to validate answers.

Keywords
Engineering mathematics, computer algebra systems.

Solving Brain Teasers/Twisters – CAS Assisted

Josef Böhm, Austria

Most of brain teasers can be faced using Mathematical Logic procedures. Therefore, using a CAS, which handles with Logic expressions, may help solving this kind of problems. The German weekly newspaper *Die Zeit* offers every week another brain teaser. Just for fun I tried to solve one or the other problem assisted by CAS. I will apply equations, Boolean expressions and other tools in order to solve the problems. It is a special challenge to produce own brain teasers.

The focus will not be directed on programming skills but on the mathematization process of the problems.

The software chosen for the presentation is my old and good friend DERIVE. I will also use TI-NspireCAS but the procedures presented can be transferred to all other CAS, of course.

Various New Methods for Computing Subresultant Polynomial Remainder Sequences (PRS's)

Alkiviadis G. Akritas

University of Thessaly, Volos, Greece, akritas@uth.gr

To the memory of Anna Johnson Pell[1] *and R. L. Gordon,*
for their inspiring Theorem of 1917![2]

Teaching subresultant prs's is an unpleasant experience because there is a misunderstanding about the role of Sylvester's two matrices and how they affect the signs of the sequences. Almost all articles and texts on the subject perform operations in $\mathbf{Z}[x]$ and use a form of pseudo-division that distorts the signs of the polynomial remainders; hence, sentences like "forget about the signs" appear quite often in the literature. In this talk we clarify the mystery about the signs and show how to compute the subresultant prs's in various ways — performing operations even in $\mathbf{Q}[x]$. Briefly stated, here is how.

Consider the polynomials $f, g \in \mathbf{Z}[x]$ of degrees n, m, respectively, with $n > m$. We call *Euclidean* prs the sequence of polynomial remainders obtained during the execution of the Euclidean algorithm for polynomial gcd. If the polynomials in the sequence are of degrees $n = m+1, m, m-1, m-2, \ldots, 0$, the sequence is called *complete*. Otherwise it is called *incomplete*.

The *complete* Euclidean prs of two polynomials can be computed either by doing polynomial divisions over the integers/rationals or by evaluating determinants of submatrices of `sylvester1` — J.J. Sylvester's matrix of 1840 [1], [12]. In the latter case, the coefficients of each polynomial remainder are the above mentioned determinants (or subresultants) and we are talking about the *subresultant* prs [6], [7], [8], [10].

Caveat 1: As demonstrated by $f = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5$ and $g = 3x^6 + 5x^4 - 4x^2 - 9x + 21$, the signs of the polynomials in an *incomplete* Euclidean prs may differ from those of the corresponding subresultant prs [3].

Analogous to Euclidean prs's are the Sturm sequences, which are obtained by *modifying* Euclid's algorithm; that is, at each step we take the negative of the remainder obtained.

Like their cousins, *complete* Sturm sequences can be computed either by doing polynomial divisions over the integers/rationals or by evaluating determinants of

[1] See the link `http://en.wikipedia.org/wiki/Anna_Johnson_Pell_Wheeler` for her biography.

[2] Discovered by Panagiotis S. Vigklas.

submatrices of `sylvester2` — J.J. Sylvester's matrix of 1853 [13]. In the latter case, the coefficients of each polynomial remainder are the *modified* subresultants and we have the *modified subresultant* prs [5].

Caveat 2: As demonstrated by $f = x^5 - 3x - 1$ and $g = 5x^4 - 3$, the signs of the polynomials in an *incomplete* Sturm sequence may differ from those of the corresponding modified subresultant prs [5].

Recall that det(`sylvester1`) defines the resultant of two polynomials and that in general det(`sylvester1`) $\neq$ det(`sylvester2`). A detailed discussion on these two matrices can be found elsewhere [4].

In 1900, E.B. Van Vleck, [14], computed *complete* Sturm sequences by triangularizing `sylvester2`. Akritas extended Van Vleck's triangularization method for *incomplete* subresultant prs's, [2], but in this case it was impossible to compute the correct sign of the polynomials in the sequence. The solution [4] came with the discovery, by Vigklas, of the Pell-Gordon theorem of 1917 [11].

In short, the Pell-Gordon theorem was a response to Van Vleck's work and is precisely the tool needed to compute the correct sign of the polynomials in an *incomplete* Sturm sequence computed with the triangularization method [5]. The only difference from what we are used today is the fact that Pell and Gordon do their computations in $\mathbf{Q}[x]$. Their theorem is stated below, whereas a detailed example can be found elsewhere [5].

Theorem (Pell-Gordon, 1917): Let

$$A = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$$

and

$$B = b_0 x^n + b_1 x^{n-1} + \cdots + b_n$$

be two polynomials of the n-th degree. Modify the process of finding the highest common factor of A and B by taking at each stage the negative of the remainder. Let the i-th modified remainder be

$$R^{(i)} = r_0^{(i)} x^{m_i} + r_1^{(i)} x^{m_i - 1} + \cdots + r_{m_i}^{(i)}$$

where $(m_i + 1)$ is the degree of the preceeding remainder, and where the first $(p_i - 1)$ coefficients of $R^{(i)}$ are zero, and the p_i-th coefficient $\rho_i = r_{p_i - 1}^{(i)}$ is different from zero. Then for $k = 0, 1, \ldots, m_i$ the coefficients $r_k^{(i)}$ are given by[3]

$$r_k^{(i)} = \frac{(-1)^{u_{i-1}} (-1)^{u_{i-2}} \cdots (-1)^{u_1} (-1)^{v_{i-1}}}{\rho_{i-1}^{p_{i-1}+1} \rho_{i-2}^{p_{i-2}+p_{i-1}} \cdots \rho_1^{p_1+p_2} \rho_0^{p_1}} \cdot \det(i, k), \tag{1}$$

[3] It is understood in (1) that $\rho_0 = b_0$, $p_0 = 0$, and that $a_i = b_i = 0$ for $i > n$.

where $\quad u_{i-1} = 1+2+\cdots+p_{i-1}, \quad v_{i-1} = p_1+p_2+\cdots+p_{i-1}$ and

$$\det(i,k) = \begin{vmatrix} a_0 & a_1 & a_2 & \cdots & \cdot & \cdot & \cdots & a_{2v_{i-1}} & a_{2v_{i-1}+1+k} \\ b_0 & b_1 & b_2 & \cdots & \cdot & \cdot & \cdots & b_{2v_{i-1}} & b_{2v_{i-1}+1+k} \\ 0 & a_0 & a_1 & \cdots & \cdot & \cdot & \cdots & a_{2v_{i-1}-1} & a_{2v_{i-1}+k} \\ 0 & b_0 & b_1 & \cdots & \cdot & \cdot & \cdots & b_{2v_{i-1}-1} & b_{2v_{i-1}+k} \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & a_0 & a_1 & \cdots & a_{v_{i-1}} & a_{v_{i-1}+1+k} \\ 0 & 0 & 0 & \cdots & b_0 & b_1 & \cdots & b_{v_{i-1}} & b_{v_{i-1}+1+k} \end{vmatrix}.$$

Proof: The proof by induction of this theorem depends on two Lemmas that can be found in the original paper of Pell and Gordon.

As indicated elsewhere [5], we use a modification of formula (1) to compute the coefficients of the Sturm sequence. In that case $p_0 = \deg(A) - \deg(B) = 1$, since B is the derivative of A and, hence, the modified formula is shown below with the changes appearing in bold:

$$r_k^{(i)} = \frac{(-1)^{u_{i-1}}(-1)^{u_{i-2}}\cdots(-1)^{u_1}(-1)^{u_0}(-1)^{v_{i-1}}}{\rho_{i-1}^{\mathbf{p_{i-1}+p_i-degDiffer}}\,\rho_{i-2}^{p_{i-2}+p_{i-1}}\cdots\rho_1^{p_1+p_2}\,\rho_0^{\mathbf{p_0}+p_1}} \cdot \frac{\det(i,k)}{\rho_{\mathbf{-1}}}, \tag{2}$$

where $\rho_{-1} = a_0$, the leading coefficient of A and `degDiffer` is the difference between the expected degree m_i and the actual degree of the remainder.

It should be noted that in our (general) case $p_0 = \deg(A) - \deg(B)$ and that the division $\frac{\det(i,k)}{\rho_{-1}}$ is possible if the leading coefficient of A is the only element in the first column of `sylvester2`. Moreover, if the leading coefficient of A is negative we work with the polynomial negated and at the end we reverse the signs of all polys in the sequence.

Using formula (2) above we were able to compute [5]:

- complete and incomplete Sturm sequences in $\mathbf{Z}[x]$ by doing divisions in $\mathbf{Q}[x]$;
- complete and incomplete *modified* subresultant prs's by evaluating the *sign* of the determinant of an appropriate submatrix of `sylvester2` — one sign computation for each polynomial.

We also wondered whether the Pell-Gordon theorem can help us compute subresultant prs's and we came up with the following rule.

The Sign/Value Rule for subresultant prs's:

To compute the exact sign of a polynomial and (possibly) adjust its value in a complete or incomplete subresultant prs we evaluate the determinant of an appropriate submatrix of `sylvester1` — one determinant computation for each polynomial.

Three new methods were developed using the above rule [3]. They have been implemented in `Sympy` and can be downloaded from `http://inf-server.inf.uth.gr/~akritas/publications/subresultants.py`.

- In the first method, `subresultants_prem2(f, g, x)`, we incorporate the new pseudo remainder function,[4] `prem2(f, g, x)`, which uses the *absolute value* of the leading coefficient of the divisor; that is, `prem2` is based on the identity $|lc(g)|^{deg(f)-deg(g)+1} \cdot f = q \cdot g + r$. This way, we preserve the "correct" sign sequence of the Euclidean prs, as discussed elsewhere [5].
- The second method, `subresultants_PG(f, g, x)`, does divisions over the rationals and uses the Pell-Gordon theorem to convert the coefficients of the polynomial remainders to integers. Here we have an implicit interplay between the two Sylvester matrices, `sylvester1` and `sylvester2`.
- Finally, in the third method, `subresultants_triang(f, g, x)`, we see — for the first time in the literature — an explicit interplay between the two Sylvester matrices, `sylvester1` and `sylvester2`. While we triangularize the latter to obtain polynomial-candidates for the subresultant prs, we evaluate determinants of submatrices of the former in order to make the candidates actual members of the prs by adjusting, if needed, their coefficients accordingly — both in value and sign!

Note that, for all three methods, the cost of computing a single subresultant per remainder is negligible if a probabilistic algorithm is available for computing large determinants — as is the case in the free computer algebra system `Xcas`. Moreover, as mentioned in [3], this cost can be further decreased if in the Sign/Value Rule — instead of `sylvester1` — we use submatrices of other, equivalent, matrices with *smaller* dimensions [9].

References

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

[4] To compute pseudo-remainders `Sympy` has the built-in function `prem(f, g, x)`, which uses the leading coefficient of the divisor along with its sign, as described in [7], [8]; that is, `prem` is based on the identity $lc(g)^{deg(f)-deg(g)+1} \cdot f = q \cdot g + r$.

[2] A.G. Akritas, *A New Method for Computing Polynomial Greatest Common Divisors and Polynomial Remainder Sequences*, Numerische Mathematik, **52**, pp. 119-127 (1988).

[3] A.G. Akritas, *Three New Methods for Computing Subresultant Polynomial Remainder Sequences (PRS's)*, Serdica Journal of Computing, to appear.

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

[5] A.G. Akritas, G.I. Malaschonok and P.S. Vigklas, *Sturm Sequences and Modified Subresultant Polynomial Remainder Sequences*, Serdica Journal of Computing, to appear.

[6] W.S. Brown and J.F. Traub, *On Euclids Algorithm and the Theory of subresultants*, Journal of the ACM, **18**, pp. 505-514 (1971).

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

[8] G.E. Collins, *Subresultants and Reduced Polynomial Remainder Sequences*, Journal of the ACM, **14**, pp. 128-142 (1967).

[9] G.M. Diaz-Toca, and L. Gonzalez-Vega, *Various New Expressions for Subresultants and Their Applications*, Applicable Algebra in Engineering, Communication and Computing, **15**, pp. 233-266 (2004).

[10] W. Habicht, *Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens*, Commentarii Mathematici Helvetici, **21**, pp. 99-116 (1948).

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

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

[13] J.J. Sylvester, *On a theory of the syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's functions, and that of the greatest algebraical common measure*, Philoshophical Transactions, **143**, pp. 407-548 (1853)

[14] E.B. Van Vleck, *On the Determination of a Series of Sturm's Functions by the Calculation of a Single Determinant*, Annals of Mathematics, Second Series, **1**(1/4), pp. 1-13 (1899 - 1900).

Teaching improper integrals with CAS

G. Aguilera[1], J.L. Galán[1], M.Á. Galán[1], Y. Padilla[1], P. Rodríguez[1], R. Rodríguez[2]

[1] *University of Málaga, Spain, jlgalan@uma.es*
[2] *Technical University of Madrid, Spain*

When teaching how to compute improper integrals such as:

$$\int_0^\infty f(t)\,\mathrm{d}t \quad ; \quad \int_{-\infty}^0 f(t)\,\mathrm{d}t \quad \text{and} \quad \int_{-\infty}^\infty f(t)\,\mathrm{d}t$$

the basic approach to compute such improper integrals is as follows:

$$\begin{aligned}
\int_0^\infty f(t)\,\mathrm{d}t &= \lim_{m\to\infty}\int_0^m f(t)\,\mathrm{d}t = \lim_{m\to\infty}\big(F(m)-F(0)\big)\\
\int_{-\infty}^0 f(t)\,\mathrm{d}t &= \lim_{m\to-\infty}\int_m^0 f(t)\,\mathrm{d}t = \lim_{m\to-\infty}\big(F(0)-F(m)\big)\\
\int_{-\infty}^\infty f(t)\,\mathrm{d}t &= \int_{-\infty}^0 f(t)\,\mathrm{d}t + \int_0^\infty f(t)\,\mathrm{d}t \quad \text{or, in case of convergence,}\\
\int_{-\infty}^\infty f(t)\,\mathrm{d}t &= \lim_{m\to\infty}\int_{-m}^m f(t)\,\mathrm{d}t = \lim_{m\to\infty}\big(F(m)-F(-m)\big)
\end{aligned}$$

(Cauchy principal value)

where F is an antiderivative of f.

But, what happens if an antiderivative F for f or the above limits do not exist?

For example, the antiderivatives for the improper integrals:

$$\int_0^\infty \frac{\sin(at)}{t}\,\mathrm{d}t \quad ; \quad \int_0^\infty \frac{\cos(at)-\cos(bt)}{t}\,\mathrm{d}t \quad \text{or} \quad \int_{-\infty}^\infty \frac{\cos(at)}{t^2+1}\,\mathrm{d}t$$

can not be computed. Hence, the above procedures cannot be used for these examples.

In this talk we will show, as an application of advanced calculus subjects, how to compute this kind of improper integrals using a CAS. Laplace and Fourier transforms or Residue Theorem in Complex Analysis are some advance techniques which can be used for this matter.

As an example of use, we will describe the file `ImproperIntegrals.mth`, developed in DERIVE 6, which deals with such computations. This utility file was first introduced at TIME 2014 Conference [1].

Some CAS use different rules for computing integrations. For example RUBI system [2], a **ru**le-**b**ased **i**ntegrator developed by Albert Rich, is a very powerful system for computing integrals using rules. We will be able to develop new rules schemes for some improper integrals using `ImproperIntegrals.mth`. These new rules can extend the types of improper integrals that a CAS can compute.

Finally, we will show some examples that we use with our students which can not be computed with the basic procedures implemented in CAS. Using the utility file `ImproperIntegrals.mth`, these examples will be easily solved.

References

[1] G. Aguilera, J.L. Galán, M.Á. Galán, Y. Padilla, P. Rodríguez and R. Rodríguez, *Advanced techniques to compute improper integrals using a* CAS, in *Proceedings of the International Conference Technology and its Integration in Mathematics Education* (TIME-2014), Krems, Austria, (2014).

[2] A.D. Rich, *Rule-based Mathematics. Symbolic Integration Rules*, in `http://www.apmaths.uwo.ca/~arich/`.

Application of wxMaxima System in LP problem of compound feed mass minimization

Włodzimierz Wojas[1], Jan Krupa[2]

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

In this paper we present application of CAS in teaching students of Warsaw University of Life Science. We apply wxMaxima system in the problem of fodders choice balancing minerals in compound feed of minimal total mass. We present procedure written in Maxima 5.26.0 which determines minimal quantities of fodders for supplying requirements of minerals for a selected type of animal.

1 Introduction

Ability to apply computational and programming tools offered by CAS systems, appears to be an important part of education in college of engineering. Students of engineering meet in the framework of core subjects a variety of practical problems: computational, optimization, data analysis and presentation, where the application of CAS systems can be very useful. Systems such as Mathematica, Maple, wxMaxima, Derive and others offer a whole range of different tools that can be used in practical engineering problems. This paper presents the application of the system wxMaxima in the problem of minimizing the mass of balanced compound feed. This problem was mandatory project for students of Agricultural and Forest Engineering at Warsaw University of Life Science within the subject Higher Mathematics II.

2 Formulation of optimization problem

The compound feed is composed of four fodders for one of the three types of animals in order to ensure daily requirements of four minerals (calcium, phosphorus, magnesium and sodium). The daily requirements of minerals for each of the three types of animals are presented in Table 1. Eleven types of fodders are presented in Table 2 together with the amounts in grams of minerals in 1kg of fodder dry matter. Students can choose four types of fodders which are combined into compound feed. After the choice of the type of animal and fodders the problem is to determine such quantities of four fodders that obtained compound feed contains acceptable amounts of minerals (for daily requirements for one head of selected type of animal) and minimize total mass of compound feed. From mathematical point of view it is a LP problem with variables representing amounts of 1kg portions of fodders combined into compound feed. But the difficulty of the task lies not in solving the LP problem. The main difficulty is to choose the fodders of the compound feed for the selected type of animal that the LP problem has feasible solution.

Table 1: Animals daily minerals requirements

	daily minerals requirements per head in grams			
Type of animals	**calcium**	**phosphorus**	**magnesium**	**sodium**
Cattle	35	15–20	12–17	4.9
Sows	13	8	1–25	3.3–3.5
Sheep	2–4	1.5–2.5	1–3	10

Table 2: Amounts of minerals (g) in 1 kg of fodder

	In 1 kg dry matter				
Index	**Fodder**	**calcium**	**phosphorus**	**magnesium**	**sodium**
1	corn	0.18	3.0	1.36	0.4
2	potatoes	0.57	1.83	1.13	0.6
3	wheat bran	1.32	13.50	5.1	1.2
4	oat	1.37	4.2	1.35	1.3
5	straw	2.43	0.79	0.80	2.8
6	linseed oil cake	3.43	11.14	5.59	1.0
7	meat meal	6.79	25.3	2.9	11.9
8	meadow hay	7.15	2.53	2.91	0.8
9	sugar beet leaves	12.40	3.1	3.9	5.5
10	alfalfa hay	18.30	2.60	2.19	0.6
11	low fat milk	12.43	9.52	1.2	6.2

Example 1. *To illustrate the problem, assume that selected type of animal is sheep. Assume also that we choose: corn, potatoes, wheat bran and oat to combine them into compound feed. Let* x_1*,* x_2*,* x_3*,* x_4 *are amounts of 1kg portions of corresponding fodders i.e. corn, potatoes, wheat bran and oat. To guarantee acceptable amounts of minerals for daily requirements and minimize total mass of compound feed, we have to solve the following LP problem:*

$$
\begin{array}{ll}
\textit{Minimize} & x_1+x_2+x_3+x_4 \\
\textit{Subject to} & 0.18x_1+0.57x_2+1.32x_3+1.37x_4 \geq 2 \\
 & 0.18x_1+0.57x_2+1.32x_3+1.37x_4 \leq 4 \\
 & 3x_1+1.83x_2+13.5x_3+4.2x_4 \leq 2.5 \\
 & 3x_1+1.83x_2+13.5x_3+4.2x_4 \geq 1.5 \\
 & 1.36x_1+1.13x_2+5.1x_3+1.35x_4 \geq 1 \\
 & 1.36x_1+1.13x_2+5.1x_3+1.35x_4 \leq 3 \\
 & 0.4x_1+0.6x_2+1.2x_3+1.3x_4 = 10 \\
 & x_i \geq 0 \, \textit{for } i = 1,2,3,4.
\end{array}
$$

Applying the standard function minimize_lp(obj, cond,[pos]) in Maxima 5.26.0 we get: no feasible solution. The answer is negative - there is no possibility to balance minerals in compound feed for these four fodders and daily requirements of minerals for sheep.

3 Numerical procedure to solve the problem

To determine feasible solution for a selected type of animal, students usually try from few to several times considering different types of fodders. This problem can be solved quite easily using optimization procedure mininimal_mass(A,b1,b2,m) which we wrote in Maxima 5.26.0 programming language. The simpler version of this problem is presented and solved using Mathematica 8.0 in paper [11]. The principles of programming in Maxima 5.26.0 are presented in [2, 3, 4, 5, 7, 8] The procedure minnimal_mass(A,b1,b2,m) is a function returning as a last component vector of pairs which first element is a number of fodder (from Table 2) and the second is the amount of this fodder combined into compound feed. If the problem has no feasible solution the function returns statement: "no feasible solution!" The amounts of fodders which we obtained have minimal total sum. A is a matrix of amounts of minerals in fodders, created on base of Table 2. b1, b2 are vectors of minimal and maximal respectively, daily requirement of minerals for selected type of animal created on base of Table 1. m is a number of fodders in compound feed. In our problem $m = 4$. Formal description of the procedure minimal_mass(A,b1,b2,m) is presented below.

Listing 1: Description of the procedure minimal_mass:

```
minimal_mass(A,b1,b2,m):=block([n,obj,p,i,L,R1,R2,R,xi,
Ai,A1,A2,T,x], /* local variables */
/* you have to load the simplex package
load("simplex"); */
n:length(A), /* n=numbers of rows in marix A */
xi:makelist(concat(x,i),i,1,m), /* xi=[x1,x2,...,xm] */
obj:sum(xi[i],i,1,m), /* obj= x1+x2+...+xm */
L:makelist(i,i,1,n), /* L=[1,2,...,xn], L is
a Maxima list */
L:setify(L), /* L={1,2,...,n}, L is Maxima set,
in order to use the function powerset */
L:powerset(L,m), /* L= all m subsets of set L */
L:full_listify(L), /* set L is converted to
a Maxima list L */
i:0, /* initial number of iterations is 0 */
T:false, /* the loop below will run at least once */
for Ai in L while is(T=false) do (
A1:makelist(A[x],x,Ai), /* Ai is a list of m positive
 integers [n_{i1},...,n_{im}], A1= m x m matrix */
R1:makelist(sum(A1[i][j]*xi[i],i,1,m)>=b1[j],j,1,m),
/* above: we construct the list of constrain
inequalities: a_1j*x_1+...+a_mj*x_m>=b1[j], j=1,2,...,m */
R2:makelist(sum(A1[i][j]*xi[i],i,1,m)<=b2[j],j,1,m),
/* above: we construct the list of constrain
inequalities: a_1j*x_1+...+a_mj*x_m<=b2[j],
j=1,2,...,m */
R:flatten([R1,R2]), /* R is a list of all constrains */
p: minimize_lp(obj,R,xi), /* we call the Maxima
function minimize_lp, the third argument xi means
that all variables in list xi are nonnegative,
p=[minimal value of object function,
[xm=value_m,...,x1=value_1] */
if (is(p#"Problem not feasible!") and is(p#"Problem
not bounded!")) then
(T:true,
p1:p, /* we save p in case we obtain minimal
feasible solution p */
p:makelist(rhs(p[2][m-i]),i,0,m-1),
/* p[2]=[xm=value_m,...,x1=value_1], so we obtain
p=[value_1,...,value_m] */
A2:Ai /* we save Ai in case we obtain minimal
feasible solution p */
),
i:i+1 /* number of iteration increased */
),
(if is(T=true) then
/* if T=true we obtain minimal feasible solution p */
[i,sol=p1,transpose(p), map(lambda([x,y],[x,y]),A2,p)]
else [i,"no nonnegative solution",p])
)$;
```

Example 2. *Assume that selected type of animal is cattle. We define A, b1, b2, m in Figure 1.*

```
A : [[0.18, 3.0, 1.36, 0.4], [0.57, 1.83, 1.13, 0.6], [1.32, 13.50, 5.1, 1.2], [1.37, 4.2,
1.35, 1.3], [2.43, 0.79, 0.80, 2.8], [3.43, 11.14, 5.59, 1.0], [6.79, 25.3, 2.9, 11.9],
[7.15, 2.53, 2.91, 0.8], [12.40, 3.1, 3.9, 5.5], [18.30, 2.60, 2.19, 0.6], [12.43, 9.52,
1.2, 6.2]]; b1 : [35, 15, 12, 4.9]; b2:[35,20,17,4.9]; m:4;
```

Figure 1: Matrix A, vectors $b1$, $b2$ and m.

The computations were conducted in Maxima5.26.0 on PC with 2.6 GHz, Pentium 4 processor and 512 Mb RAM under Windows XP platform. Maxima elapsed_run_time was 0.07 s. The final result is presented in Figure 2.

$$
\begin{gathered}
[5, sol = [6.191975412126295, [x4 = 4.737686504610226,\\
x3 = 0.3954624196703, x2 = 1.058826487845771, x1 = 0]],\\
\begin{pmatrix} 0 \\ 1.058826487845771 \\ 0.3954624196703 \\ 4.737686504610226 \end{pmatrix},\\
[[1,0],[2,1.058826487845771],[3,0.3954624196703],[8,4.737686504610226]]]
\end{gathered}
$$

Figure 2: Final solution of the problem.

This solution was obtained in fifth iteration. First four iterations had no feasible solutions. The obtained result gives us the following amounts of fodders (see column Index in Table 2) : $[1,0]$ *means: 0.0000 kg of meadow,* $[2,1.0588]$ *means 1.0588 kg of wheat bran,* $[3,0.3955]$ *means 0.3955 kg of potatoes and* $[8,4.7377]$ *means 4.7377 kg of corn. Total mass of compound feed is 6.192 kg. It is minimal* *mass of compound feed comprised of these four fodders which guarantees daily requirement of four minerals for one cattle.*

The procedure minimal_mass(A,b1,b2,m) can be easily extended to minimize total mass of compound feed among all possible compound feeds balancing minerals for selected type of animal. The extended procedure is in Figure Listing 2

Listing 2: Description of the procedure minimal_mass1:

```
minimal_mass1(A,b1,b2,m):=block([n,obj,p,p1,p0,i,i0,L,
R1,R2,R,xi, Ai,A1,A2,T,x,y0],
n:length(A),
xi:makelist(concat(x,i),i,1,m),
obj:sum(xi[i],i,1,m),
L:makelist(i,i,1,n),
L:setify(L),
L:powerset(L,m),
L:full_listify(L),
i:0,
i0:0,
y0:100,
T:false,
for Ai in L do (
/* in minimal_mass we have: for Ai in L while is(T=false):
now the condition "while is(T=false)" is not needed */
A1:makelist(A[x],x,Ai),
R1:makelist(sum(A1[i][j]*xi[i],i,1,m)>=b1[j],j,1,m),
R2:makelist(sum(A1[i][j]*xi[i],i,1,m)<=b2[j],j,1,m),
R:flatten([R1,R2]),
p: minimize_lp(obj,R,xi),
if (is(p#"Problem not feasible!") and is(p#"Problem
not bounded!")) then
(T:true,
if is(p[1]<y0) then (
y0:p[1],
p1:p,
p0:makelist(rhs(p[2][i]),i,1,m),
A2:Ai,
i0:i
)),
i:i+1
),
(if is(T=true) then
[i, i0, sol=p1,transpose(p0), map(lambda([x,y],[x,y]),A2,p0)]
else [i,"no nonnegative solution",p0])
);
```

The computations were conducted in Maxima5.26.0 on PC with 2.6 GHz, Pentium 4 processor and 512 Mb RAM under Windows XP platform. Maxima elapsed_run_time was 1.83 s. The final result is presented in Figure 3.

Applying the procedure minimal_mass1(A,b1,b2,m) to the extension of the problem for cattle we obtain the solution presented in Figure 3.

$$\begin{gathered}
[330,321,sol=[3.108826328073963,[x4=1.325453353602,\\
x3=0.51585666963707,x2=0,x1=1.267516304834889]],\\
\begin{pmatrix} 1.325453353602 \\ 0.51585666963707 \\ 0 \\ 1.267516304834889 \end{pmatrix}\\
[[6,1.325453353602],[8,0.51585666963707],[9,0],[10,1.267516304834889]]]
\end{gathered}$$

Figure 3: Final solution of the generalized problem with cattle.

This solution was obtained in 321-th iteration. First 320 iterations give no feasible solutions or feasible solutions with value of object function greater than 3.1088. The obtained result gives us the following amounts of fodders (see column Index in Table 2): $[6,1.32545]$ means: 1.32545 kg of linseed oil cake, $[8,0.515856669637]$ means 0.515856669637 kg of meadow hay, $[9,0]$ means 0.0000 kg of sugar beet leaves and $[10,1.2675163]$ means 1.2675163 kg of alfalfa hay. Total mass of compound feed is 3.1088 kg. It is minimal mass of compound feed comprised of these four fodders chosen from all eleven fodders, which guarantees daily requirement of four minerals for one cattle.

4 Summary

In this paper the procedure minimal_mass(A,b1,b2,m) implemented in Maxima 5.26.0 was presented. This procedure solves the problem of fodders choice for minimal mass compound feed in order to ensure daily requirement of four minerals (calcium, phosphorus, magnesium and sodium) for a selected type of animal. This problem was assignment for students Agricultural and Forest Engineering at

Warsaw University of Life Science. Finding solution of the problem students need quite much of work considering various selection of four fodders in order to obtain balancing minerals in compound feed. Applying CAS system such as wxMaxima allows find solution of described above problem in a much less time.

References

[1] Homepage of the Maxima Project: http://maxima.sourceforge.net

[2] *Maxima Documentation* at http://maxima.sourceforge.net/documentation.html.

[3] *Maxima 5.36.0 Manual* at http://maxima.sourceforge.net/docs/manual/maxima.html.

[4] Edwin L. Woollett, *Maxima by Example* at http://web.csulb.edu/ woollett/#mbe

[5] Rafał Topolnicki, *Maxima - practical guide* (in polish) at http://www.knf.ifd.uni.wroc.pl/materialy/maxima.pdf

[6] Robert Dodier, *Minimal Maxima* at http://maxima.sourceforge.net/docs/tutorial/en/minimal-maxima.pdf

[7] Paulo Ney de Souza, Richard J. Fateman, Joel Moses, Cliff Yapp, *The Maxima Book* at http://maxima.sourceforge.net/docs/maximabook/maximabook-19-Sept-2004.pdf

[8] Gilberto E. Urroz, *MAXIMA: Science and Engineering Applications* at http://www.neng.usu.edu/cee/faculty/gurro/Maxima.html

[9] Jaime E. Villate, *Dynamical systems* (in Portuguese) at http://www.villate.org/doc/sistemasdinamicos/sistdinam-1_2.pdf

[10] Homepage of the wxMaxima Project: http://andrejv.github.io/wxmaxima/

[11] Włodzimierz Wojas, Jan Krupa, *Application of Mathematica System in the problem of balance of ingredients for compound feed*, Computer Algebra Systems In Teaching and Research 2013, Vol. 4, No 1, pp. 278-282

[12] Ziołecka A., Kużdowicz M., Chomszyn M. *Tables of ingriedients of domestic fodders* (in polish) PWN Warszawa (1987)

[13] The minerals in animal nutrition. Poznan University of Life Science (1994) (in polish)

[14] www.dodatkipaszowe.pl

The Use of CAS for Logical Analysis in Mathematics Education

T. Takahashi[1], T. Sakai[2], F. Iwama[1]

[1]*Konan University, Japan, takahasi@konan-u.ac.jp*
[2]*Naruto Normal University, tsakai@naruto-u.ac.jp*

In mathematics education, ascertaining the concepts of given domains in terms of conceptual and procedural knowledge is essential as a mechanism of knowledge change during knowledge acquisition. Conceptual knowledge consists of an implicit or explicit system of interlinked pieces of knowledge for a given domain, and procedural knowledge comprises systems of multiple execution series for problem solution [1], [2]. The concept of ratio is applied in ascertaining the relation between two quantities and in comparing the relative quantities of two sets. It differs in meaning from simple multiplication and is active in the sense of comparing the relative sizes of given quantities and base quantities rather than directly comparing quantities [3]. So, we focused on comparison of the relations between quantities in two different sets. It has been noted that the concept of ratio can be investigated in a fairly pure form as a logical mathematical recognition [4], and we treated this comparison as a probabilistic comparison task. Ratio and probability are different concepts, but for children unschooled in probability, the ratio concept can be utilized as an approach for probability settings. We consider these problems using theorem prover.

Computer algebra systems are being used frequently in mathematics education. Although good teaching examples and experiences exist, it is clear that the efficient and successful use is not self-evident. A subtle relationship exists between paper-and-pencil techniques, computer algebra systems, and conceptual understanding. The nature of computer systems is different from that of paper-and-pencil techniques. Using a computer algebra system requires insight into procedures as well as into the concepts involved. In addition, the way computer manages the procedures can affect mathematical concepts.

Use of a computer algebra system with a theorem prover can correct the weakness in mathematics education. We can clearly understand mathematical concepts and can minimize the burden of operation opportunities. Computer algebra systems using a theorem prover bring about serious changes in mathematics education. A theorem prover *Theorema* uses a computer algebra system, but reduces the operations of the computer algebra system. Therefore, learners can concentrate on mathematical problems.

In this study, we applied propositional and predicate logic for mathematical explication of the processes of inference by using theorem prover *Theorema* [5] is a Mathematica package (a collection of packages, in fact) that provides a mathematical assistant system (MAS) inside of and based on Mathematica. A MAS supports the user in formulating and structuring of mathematical knowledge, proving mathematical statements, formulating and executing mathematical algorithms, performing computations, etc. *Theorema* allows you to express algorithms using the language of predicate logic or parts of the Mathematica programming language supporting procedural programming, most importantly various forms of loops. *Theorema* allows you to organize mathematical knowledge as hierarchies of interdependent theories. By settling the definitions, we can continue and try to prove some properties of the newly defined entities.

When considering a human model, the model must be viewed as a process model, as a knowledge model, and as a control model. We can consider that such an approach has been applied to the understanding of theorem proving. A computer algebra system with a theorem prover is being developed. We must consider the theorem prover from mathematical studies. This research aims at extending current computer systems using facilities for supporting mathematical proving. The system consists of a general higher-order predicate logic prover and a collection of special provers. The individual provers imitate the proof style of human mathematicians and produce human-readable proofs in natural language presented in nested cells.

To do mathematics is gaining knowledge and solving problems by reasoning. Theorem prover *Theorema* is a powerful tool for learning mathematics.

References

[1] J. Hiebert and P. Lefevre, " Conceptual and Procedural Knowledge in Math-ematics: An Introductory Analysis ", in J. Hiebert (ed.), Conceptual and Procedural Knowledge: The Case of Mathematics, Hillsdale, N. J.: Lawrence Erlbaum Associates, pp.1-27 (1986).

[2] B. Rittle-Johnson, R. S. Siegler, and N. W. Alibali, " Developing Conceptual Understanding and Procedural Skill in Mathematics: An Iterative Process ", Journal of Educational Psychology, Vol.93, No.2, pp.346-362 (2001).

[3] R. Maeda, " Concept of the Ratio ", New Arithmetic Education Lecture Vol. 3: Mathematical Relations, in C. Akahane (ed.), Yoshino-shobo Publishing Ltd, pp.239-247 (1960) (in Japanese).

[4] A. Nakagaki, " How do Children Judge the Size of the Ratio? -The Developmental Study ", Research report of the National Institute for Educational Research, Vol.13, pp.35-55 (1986) (in Japanese).

[5] https://www.risc.jku.at/research/theorema/software/documentation/tutorial/TheTheoremaSystem.html

Indexed elementary functions in Maple

David Jeffrey
University of Western Ontario, Canada

Multi-branched functions cause troubles for mathematicians (particularly students) and computers. I present implementations of the inverses of the elementary functions sin,cos,tan,exp, ^m which handle the branches by labelling them. The new functions are more elegant, easier to work with and easier to understand. At least that is what I think.

Computer Algebra in Coding Theory and Cryptography

Session Organizers

Irene Márquez-Corbella
INRIA - Paris
irene.marquez-corbella@inria.fr

Ruud Pellikaan
Dep. of Mathematics and Computing Science
Eindhoven University of Technology
G.R.Pellikaan@tue.nl

Overview

This session aims to bring together researchers from all areas related to computer algebra (both theoretical and algorithmic) applied to Coding theory and Cryptography.

Since much of the work related to these topics is recent or is still ongoing, this session will provide a stimulating forum where experts will be able to not only report their recent results, but also to propose new lines of research and discuss open questions.

Trial set and Gröbner bases for binary codes

M. Borges-Quintana[1a], M. A. Borges-Trenard[2], Edgar Martínez Moro[3]

[1 2] *Department of Mathematics, Faculty of Mathematics and Computer Science, University of Oriente, Santiago de Cuba, Cuba, mijail@csd.uo.edu.cu, mborges@csd.uo.edu.cu*
[3] *Institute of Mathematics IMUVa, University of Valladolid. Valladolid, Castilla, Spain, edgar@maf.uva.es*

We show the connections between trial sets and Gröbner bases for binary codes, which gives more characterizations of trial sets in the context of Gröbner bases and algorithmic ways for compute them. In this sense, minimal trial set are characterized as trial sets associated with minimal Gröbner bases.

The concept of trial set was introduced in [6]. This set of codewords can be used to derive and algorithm for doing complete decoding in a similar way that a gradient decoding algorithm uses a test set (see [1]). A trial set allows to characterize the so called *correctable errors* and to investigate the monotone structure of correctable and uncorrectable errors, also important bounds on the error-correction capability of binary codes beyond half of minimum distance using trial sets are presented in [6]. One problem posted in the conclusion of [6] was the importance of charactherize minimal trial sets for families of binary codes.

The ideal associated with any linear code (code ideal for simplicity) was introduced in [2] together with applications of Gröbner bases theory in this context, such that the reduction process by Gröbner bases of code ideals w.r.t. to specific orders corresponds to the decoding process of the code.

In Section 1 we give the main concepts and results related with binary codes, trial sets, the code ideals and Gröbner bases which are needed for an understanding of this work. The connection between trial sets for binary codes and Gröbner bases for the corresponding code ideal is presented in Section 2. The main results in this contribution are Proposition 2, Theorems 4 and 5, and the subsection 2.1 about minimal trial sets and minimal Gröbner bases.

1 Preliminaries

Binary codes

By $\mathbb{Z}$, $\mathbb{K}$, $\mathbb{K}[\mathbf{X}]$ and $\mathbb{F}_2$ we denote the ring of integers, an arbitrary field, the polynomial ring in n variables over the field $\mathbb{K}$ and the finite field with 2 elements.

[a] Supported by a Post-doctorate scholarship at the University of Valladolid (09-2014 to 02-2015) by Erasmus Mundus Program, Mundus Lindo Project.

A *binary linear code* $\mathscr{C}$ over $\mathbb{F}_2$ of length n and dimension k, or an $[n,k]$ binary code for short, is a k-dimensional subspace of $\mathbb{F}_2^n$. We will call the vectors $\mathbf{v}$ in $\mathbb{F}_2^n$ words and in the particular case where $\mathbf{v} \in \mathscr{C}$, codewords. For every word $\mathbf{v} \in \mathbb{F}_2^n$ its *support* is defined as $\operatorname{supp}(\mathbf{v}) = \{i \mid v_i \neq 0\}$ and its *Hamming weight*, denoted by $\mathrm{w}_H(\mathbf{v})$ as the cardinality of $\operatorname{supp}(\mathbf{v})$.

The *Hamming distance*, between two vectors $\mathbf{x},\ \mathbf{y} \in \mathbb{F}_2^n$ is $d_H(\mathbf{x},\mathbf{y}) = \mathrm{w}_H(\mathbf{x}-\mathbf{y})$. The *minimum distance* $d(\mathscr{C})$ of a linear code $\mathscr{C}$ is defined as the minimum weight among all nonzero codewords.

For the rest of this section we follow [6]. We will consider $\prec$ a so called α-ordering on $\mathbb{F}_2^n$ (a weight compatible total ordering on $\mathbb{F}_2^n$) which is monotone:

$$\left.\begin{array}{l}\text{for any } \mathbf{y}_1, \mathbf{y}_2 \; s.t.\; 2 \leq \mathrm{w}_H(\mathbf{y}_1) = \mathrm{w}_H(\mathbf{y}_1) < n \text{ and } \operatorname{supp}(\mathbf{y}_1) \cap \operatorname{supp}(\mathbf{y}_1) \neq \emptyset \\ \text{and for any } i \in \operatorname{supp}(\mathbf{y}_1) \cap \operatorname{supp}(\mathbf{y}_1) \text{ and vectors } \mathbf{x}_1 \text{ and } \mathbf{x}_2 \text{ defined by} \\ \operatorname{supp}(\mathbf{x}_1) = \operatorname{supp}(\mathbf{y}_1) \setminus \{i\} \text{ and } \operatorname{supp}(\mathbf{x}_2) = \operatorname{supp}(\mathbf{y}_2) \setminus \{i\} \text{ then } \mathbf{y}_1 \prec \mathbf{y}_2 \text{ if} \\ \mathbf{x}_1 \prec \mathbf{x}_2. \end{array}\right\} \quad (1)$$

The set of correctable errors of a binary code $\mathscr{C}$ ($E^0(\mathscr{C})$) are the minimal elements w.r.t. $\prec$ in each coset of $\mathbb{F}_2^n/\mathscr{C}$, and the elements of $E^1(\mathscr{C}) = \mathbb{F}_2^n \setminus E^0(\mathscr{C})$ are called uncorrectable errors. A *trial set* $T \subset \mathscr{C} \setminus \mathbf{0}$ of the code $\mathscr{C}$ is a set which has the property $\mathbf{y} \in E^0(\mathscr{C})$ if and only if $\mathbf{y} \leq \mathbf{y}+\mathbf{c}$, for all $\mathbf{c} \in T$.

Note that with a trial set we obtain an algorithm which returns the corresponding correctable error for a received word $\mathbf{y}$. Since we choose a monotone α-ordering on $\mathbb{F}_2^n$, the set of correctable and uncorrectable errors form a monotone structure, namely, that if $\mathbf{x} \subset \mathbf{y}$, then $\mathbf{x} \in E^1(\mathscr{C})$ implies $\mathbf{y} \in E^1(\mathscr{C})$ and $\mathbf{y} \in E^0(\mathscr{C})$ implies $\mathbf{x} \in E^0(\mathscr{C})$.

Let $M^1(\mathscr{C})$ be the set of minimal uncorrectable errors i.e. the set of $\mathbf{y} \in E^1(\mathscr{C})$ such that, if $\mathbf{x} \subseteq \mathbf{y}$ and $\mathbf{x} \in E^1(\mathscr{C})$, then $\mathbf{x} = \mathbf{y}$. In a similar way, the set of maximal correctable errors is the set $M^0(\mathscr{C})$ of elements $\mathbf{x} \in E^0(\mathscr{C})$ such that, if $\mathbf{x} \subseteq \mathbf{y}$ and $\mathbf{y} \in E^0(\mathscr{C})$, then $\mathbf{x} = \mathbf{y}$.

For $\mathbf{c} \in \mathscr{C} \setminus \mathbf{0}$, a *larger half* is defined as a minimal word $\mathbf{u}$ in the ordering $\preceq$ such that $\mathbf{u}+\mathbf{c} \prec \mathbf{u}$. The set of larger halves for a codeword $\mathbf{c}$ is denoted by $\mathrm{L}(\mathbf{c})$, and for $U \subseteq \mathscr{C} \setminus \mathbf{0}$ the set of larger halves for elements of U is denoted by $\mathrm{L}(U)$. Note that $\mathrm{L}(\mathscr{C}) \subseteq E^1(\mathscr{C})$.

For any $\mathbf{y} \in \mathbb{F}_2^n$, let $H(\mathbf{y}) = \{c \in \mathscr{C} : \mathbf{y}+\mathbf{c} \prec \mathbf{y}\}$, and we have $\mathbf{y} \in E^0(\mathscr{C})$ if and only if $H(\mathbf{y}) = \emptyset$, and $\mathbf{y} \in E^1(\mathscr{C})$ if and only if $H(\mathbf{y}) \neq \emptyset$. Theorem 1 of [6] provides a characterization of the set $M^1(\mathscr{C})$ in terms of $H(\cdot)$ and larger halves of the set of minimal codewords $M(\mathscr{C})$.

Proposition 1 (Corollary 3, [6]) *Let $\mathscr{C}$ be a binary code and $T \subseteq \mathscr{C} \setminus \mathbf{0}$. The following statements are equivalent:*

1. *T is a trial set for $\mathscr{C}$.*

2. *If $\mathbf{y} \in M^1(\mathscr{C})$, then $T \cap H(\mathbf{y}) \neq \emptyset$.*

3. *$M^1(\mathscr{C}) \subseteq \mathrm{L}(T)$.*

Gröbner bases and binary codes

We define the following characteristic crossing function: $\Delta : \mathbb{F}_2^s \longrightarrow \mathbb{Z}^s$ which replace the class of $0, 1$ by the same symbols regarded as integers. This map will be used with matrices and vectors acting coordinate-wise. Also, for the reciprocal case, we defined $\nabla : \mathbb{Z}^s \longrightarrow \mathbb{F}_2^s$. Let $\mathbf{X}$ denotes n variables $x_1, \ldots, x_n$ and let $\mathbf{a} = (a_1, \ldots, a_n)$ be an n-tuple of elements of the field $\mathbb{F}_2$. We will adopt the following notation:

$$\mathbf{X}^{\mathbf{a}} := x_1^{\Delta a_1} \cdots x_n^{\Delta a_n} \in [\mathbf{X}]. \tag{2}$$

The code ideal can be given by the two equivalent formulas in (3) and (4) below, the equivalency between (3) and (4) was proved in [4]. Let W be a generator matrix of an $[n, k]$ binary code $\mathscr{C}$ (the row space of the matrix generates $\mathscr{C}$) and $\mathbf{w}_i$ denotes its rows for $i = 1, \ldots k$.

$$I(\mathscr{C}) = \left\langle \mathbf{X}^{\mathbf{a}} - \mathbf{X}^{\mathbf{b}} \mid \mathbf{a} - \mathbf{b} \in \mathscr{C} \right\rangle \subseteq \mathbb{K}[\mathbf{X}]. \tag{3}$$

$$I(\mathscr{C}) = \left\langle \{\mathbf{X}^{\mathbf{w}_i} - 1 : i = 1, \ldots k\} \cup \{x_i^2 - 1 : i = 1, \ldots, n\} \right\rangle \subseteq \mathbb{K}[\mathbf{X}]. \tag{4}$$

Note that $I(\mathscr{C})$ is a zero-dimensional ideal since the quotient ring $R = \mathbb{K}[\mathbf{X}]/I(\mathscr{C})$ is a finite dimensional vector space and its dimension is equal to the number of cosets in $\mathbb{F}_2^n/\mathscr{C}$.

For every element $\mathbf{X}^a$ in the monoid $[\mathbf{X}]$, with $a \in \mathbb{N}^n$, we have a corresponding vector $\nabla(a) \in \mathbb{F}_2^n$, and viceversa, any vector $\mathbf{w} \in \mathbb{F}_2^n$ has a unique standard representation[b] $\mathbf{X}^{\mathbf{w}}$ as an element of $[\mathbf{X}]$ (see (2)).

Let $<$ be a term order, let us $\mathrm{T}(f)$ denotes the maximal term of a polynomial f with respect to the order $<$. The set of maximal terms of the set $F \subseteq K[X]$ is denoted $\mathrm{T}\{F\}$ and $\mathrm{T}(F)$ denotes the semigroup ideal generated by $\mathrm{T}\{F\}$. Finally, $\langle F \rangle$ is the polynomial ideal in $\mathbb{K}[\mathbf{X}]$ generated by F. In particular, for the code ideal $I(\mathscr{C})$, $\mathrm{T}(I(\mathscr{C}))$ is the set of maximal terms and $N(I(\mathscr{C})) = [\mathbf{X}] \setminus \mathrm{T}(I(\mathscr{C}))$ the set of canonical forms. We emphasize that there is a one to one correspondence between the set of canonical forms and the cosets in $\mathbb{F}_2^n/\mathscr{C}$. One characterization of Gröbner bases is that G is a *Gröbner basis* of the ideal $\langle \mathrm{G} \rangle$ if and only if $\mathrm{T}(\langle \mathrm{G} \rangle) = \mathrm{T}(\mathrm{G})$.

[b] The exponents of the variables are 0 or 1.

2 Gröbner bases and trial set for binary codes

It is not difficult to see also the conection between total degree orders $<$ on $[\mathbf{X}]$ and α-orderings monotone $\prec$ on $\mathbb{F}_2^n$. In essence, any total degree compatible ordering induces an α-ordering monotone $\prec$ on $\mathbb{F}_2^n$ such that $\mathbf{v} \prec \mathbf{w}$ if $\mathbf{X}^{\mathbf{v}} < \mathbf{X}^{\mathbf{w}}$ for any $\mathbf{v}, \mathbf{w} \in \mathbb{F}_2^n$. On the other hand, given an α-ordering monotone on $\mathbb{F}_2^n$ we could define a total ordering on $[\mathbf{X}]$ which is not admisible, a class of these orders on $[\mathbf{X}]$ were called in [2] error-vector orderings.

In this work we will focus in the first situation, the α-ordering monotone which is defined in [6] it is derived from the Graduated Lexicographical order. In general, let $<$ be a total degree term order on $[\mathbf{X}]$, and let $\prec$ be the corresponding α-ordering monotone on $\mathbb{F}_2^n$.

Proposition 2 [Correctable and uncorrectable errors and canonical forms and maximal terms] *Let $X^{\mathbf{w}} \in [\mathbf{X}]$, $\mathbf{w} \in \mathbb{N}^n$ then*

1. *If $X^{\mathbf{w}}$ is not the standard representation of the word $\nabla(\mathbf{w})$ in $\mathbb{F}_2^n$, then it is a maximal term i.e. $X^{\mathbf{w}} \in \mathrm{T}(I(\mathscr{C}))$.*

2. *If $\nabla(\mathbf{w}) \in E^1(\mathscr{C})$, then $X^{\mathbf{w}} \in \mathrm{T}(I(\mathscr{C}))$.*

3. *If $X^{\mathbf{w}}$ is the standard representation of the word $\nabla(\mathbf{w})$ and $\nabla(\mathbf{w}) \in E^0(\mathscr{C})$, then $X^{\mathbf{w}}$ is a canonical form i.e. $X^{\mathbf{w}} \in N(I(\mathscr{C}))$.*

4. *If $X^{\mathbf{w}}$ is the standard representation of the word $\nabla(\mathbf{w})$ and $\nabla(\mathbf{w}) \in M^1(\mathscr{C})$, then $X^{\mathbf{w}}$ is an irredundant maximal term, i.e. $X^{\mathbf{w}} \notin \mathrm{T}(I(\mathscr{C})) \setminus \{X^{\mathbf{w}}\}$ and is a maximal term of any Gröbner basis. The set of irredundant maximal terms are the maximal terms of any minimal Gröbner basis, for example, of the reduced Gröbner basis.*

For simplicity, we will assume that the coefficients of the maximal terms in a Gröbner basis are positive.

Definition 3 (Gröbner codewords [3]) *Let* G *be a Gröbner basis for $I(\mathscr{C})$ w.r.t. $<$, the set of Gröbner codewords $\mathscr{C}_{\mathrm{G}}$ corresponding to* G *are the codewords associated with* G *by $\mathscr{C}_{\mathrm{G}} = \{\mathbf{c} \in \mathscr{C} : \mathbf{c} = \mathbf{w} + \mathbf{v},$ s.t. $X^{\mathbf{w}} - X^{\mathbf{v}} \in \mathrm{G}, \mathbf{w}, \mathbf{v} \in \mathbb{F}_2^n, \mathbf{v} \prec \mathbf{w}\}$.*

Theorem 4 *Let* G *be a Gröbner basis for $I(\mathscr{C})$ w.r.t. $<$, then $\mathscr{C}_{\mathrm{G}}$ is a trial set.*

Proof. We will prove the stament 2 in Proposition 1. Let $\mathbf{w} \in M^1(\mathscr{C})$, then $X^{\mathbf{w}} \in \mathrm{T}(\mathrm{G})$ (see Proposition 2.4) and there exists $\mathbf{c} \in \mathscr{C}_{\mathrm{G}}$ s.t. $\mathbf{c} = \mathbf{w} + \mathbf{v}$ s.t. $\mathbf{v} \prec \mathbf{w}$. Thus $\mathbf{c} + \mathbf{w} = \mathbf{v} \prec \mathbf{w}$ and $\mathbf{c} \in H(\mathbf{w})$.

Theorem 5 *Let T be a trial set, the set* $\mathrm{G}_T = \{\mathbf{X}^{\mathbf{w}} - \mathbf{X}^{\mathbf{v}} : \mathbf{w} \in \mathrm{L}(\mathbf{c})$ *for some* $\mathbf{c} \in T$ *and* $\mathbf{v} = \mathbf{c} - \mathbf{w}\} \cup \{x_i^2 - 1 : i = 1, \ldots, n\}$ *is a Gröbner basis for $I(\mathscr{C})$ w.r.t. $<$.*

Proof. If $X^{\mathbf{u}}$ is a maximal term which is not the standard representation of $\nabla(\mathbf{u})$, then it can be reduced to the standard representation of $\nabla(\mathbf{u})$ by means of the set $\{x_i^2 - 1 : i = 1, \ldots, n\}$. Thus, let us assume that $X^{\mathbf{u}} \in \mathrm{T}(I(\mathscr{C}))$ and $\mathbf{u} \in E^1(\mathscr{C})$. It is clear that there exists $\mathbf{w} \subseteq \mathbf{u}$ s.t. $\mathbf{w} \in M^1(\mathscr{C})$, $\mathbf{w} \in M^1(\mathscr{C})$ implies there exists $\mathbf{c} \in T$ s.t. $\mathbf{w} \in \mathrm{L}(\mathbf{c})$ (by Proposition 1.3). Let $\mathbf{v} = \mathbf{c} - \mathbf{w}$, then we have $\mathbf{X}^{\mathbf{w}} - \mathbf{X}^{\mathbf{v}} \in \mathrm{G}_T$ and $\mathbf{X}^{\mathbf{w}} \mid \mathbf{X}^{\mathbf{u}}$ (remember $\mathbf{w} \subseteq \mathbf{u}$). Consequently, G_T is a Gröbner basis for $I(\mathscr{C})$.

2.1 Minimal trial sets and minimal Gröbner bases

A minimal trial set is a trial set such that any strictly subset is not a trial set. Having an smaller trial set, it is an smaller set that it is used for decoding in order to compute the corresponding correctable error to a received word, althought smaller trial sets do not necessaryly ensure more efficiency. In [6] is given a main advantage of having a minimal trial set, because the size of trial sets are used to derive some important bounds on the error correction beyond half the minimum distance.

By Proposition 1.3, the set of larger halves of a trial set T should contains at least the set $M^1(\mathscr{C})$, by Theorem 5 and Proposition 2.4 this means that the corresponding Gröbner basis G_T should coontains at least the irredundant maximal terms (it is the case for any Gröbner basis); therefore, there is a direct connection between minimal trial sets and minimal Gröbner bases. In particular, a distinguished minimal trial set would be the set of Gröbner codewords corresponding to the reduced Gröbner basis.

References

[1] A. Barg, *Complexity issues in coding theory*, in *Handbook of coding theory*, **I**, North-Holland, Amsterdam, pp. 649-754 (1998).

[2] M. Borges-Quintana, M.A. Borges-Trenard and E. Martínez-Moro, *On a Gröbner bases structure associated to linear codes*, J. Discret. Math. Sci. Cryptogr, **10(2)**, pp. 151-191 (2007).

[3] M. Borges-Quintana, M.A. Borges-Trenard and E. Martínez-Moro, *A Gröbner representation for linear codes*, in *Advances in coding theory and cryptography, Ser. Coding Theory Cryptol.*, **3**, World Sci. Publ., Hackensack, NJ, pp. 17-32, (2007).

[4] M. Borges-Quintana, M.A. Borges-Trenard, P. Fitzpatrick and E. Martínez-Moro, *Gröbner bases and combinatorics for binary codes*, Appl. Algebra Engrg. Comm. Comput., **19(5)**, pp. 393-411 (2008).

[5] W.C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge (2003).

[6] T. Helleseth, T. Kløve and I.L. Vladimir, *Error-correction capability of binary linear codes*, IEEE Transactions on Information Theory, **51(4)**, pp. 1408-1423 (2005).

Geometric and Computational Approach to Classical and Quantum Secret Sharing

Ryutaroh Matsumoto[1], Diego Ruano[2]

[1] *Tokyo Institute of Technology, Japan, ryutaroh@rmatsumoto.org*
[2] *Aalborg University, Denmark, diego@math.aau.dk*

1 Introduction

Secret sharing (SS) [15] is a cryptographic scheme to encode a secret to multiple shares being distributed to participants, so that only qualified (or authorized) sets of participants can reconstruct the original secret from their shares. Traditionally both secret and shares were classical information (bits). Several authors [5, 7, 16] extended the traditional SS to a quantum one so that a quantum secret can be encoded to quantum shares.

When we require unqualified sets of participants to have zero information of the secret, the size of each share must be larger than or equal to that of the secret. By tolerating partial information leakage to unqualified sets, the size of shares can be smaller than that of the secret. Such an SS is called a ramp (or non-perfect) SS [2, 13, 17]. The quantum ramp SS was proposed by Ogawa et al. [14]. In their construction [14] as well as its improvement [18], the size of shares can be L times smaller relative to quantum secret than its previous construction [5, 7, 16], where L is the number of qudits in quantum secret.

Classical secret sharing is said to be linear if a linear combination of shares corresponds to the linear combination of the original secrets [4]. It is also known that every linear ramp secret sharing can be expressed by a nested pair of linear codes $C_2 \subset C_1 \subset \mathbf{F}_q^n$. On the other hand, a nest code pair $C_2 \subset C_1 \subset \mathbf{F}_q^n$ can also give a quantum secret sharing as described in [10]. A share set is said to be forbidden if it has no information about the secret. It is natural to express conditions for qualified and forbidden sets in terms of $C_2 \subset C_1$, and the following is known:

Theorem 1 *[1, 9, 10] Let $J \subseteq \{1, \ldots, n\}$, and define $P_J : \mathbf{F}_q^n \to \mathbf{F}_q^{|J|}$, $(x_1, \ldots, x_n) \mapsto (x_j : j \in J)$. We consider classical and quantum secret sharing constructed from $C_2 \subset C_1$. J can be regarded as a share set, and J is qualified in the classical secret sharing if and only if*

$$\dim P_J(C_1)/P_J(C_2) = \dim C_1/C_2, \tag{1}$$

and J is forbidden in the classical secret sharing if and only if

$$P_J(C_1) = P_J(C_2). \tag{2}$$

Let $\overline{J} = \{1, \ldots, n\} \setminus J$. In the quantum secret sharing, J is qualified if and only if

$$\text{both} \left\{ \begin{array}{l} \text{(1) is true,} \\ P_{\overline{J}}(C_1) = P_{\overline{J}}(C_2) \end{array} \right. \quad \text{i.e.,} \left\{ \begin{array}{l} J \text{ is classically qualified,} \\ \overline{J} \text{ is classically forbidden} \end{array} \right. \tag{3}$$

hold, and J is forbidden if and only if $\overline{J}$ is qualified.

Since C_1 and C_2 are linear codes, it is natural to use algebraic geometry codes to construct C_1 and C_2 [3]. Let F be an algebraic function field of one variable with genus $g(F)$, P_1, …, P_n its rational places, $G_1 \geq G_2$ divisors whose support contain none of P_1, …, P_n. Define $C(P_1 + \cdots + P_n,\, G_1) = \{(f(P_1),\, \ldots,\, f(P_n)) \mid f \in \mathscr{L}(G_1)\}$. By the Riemann-Roch theorem, for $C_1 = C(P_1 + \cdots + P_n,\, G_1)$ and $C_2 = C(P_1 + \cdots + P_n,\, G_2)$, it is straightforward to see

Theorem 2 *Equation (1) holds if*

$$|J| \geq 1 + \deg G_1. \tag{4}$$

Equation (2) holds if

$$|J| \leq \deg G_2 - 2g(F) + 1. \tag{5}$$

Equation (3) holds if

$$|J| \geq \max\{1 + \deg G_1, n - (\deg G_2 - 2g(F) + 1)\}. \tag{6}$$

The purpose of this note is to find sufficient conditions **less** demanding than (4)–(6) by using geometric properties of the set of points $\{P_j \mid j \in J\}$.

2 Geometric and Computational Analysis of Qualified and Forbidden Sets

2.1 Computational Approach

Fix a rational place Q arbitrarily. When $C_1 = C(P_1 + \cdots + P_n,\, G_1)$ and $C_2 = C(P_1 + \cdots + P_n,\, G_2)$, (1) holds

$$\begin{aligned}
&\Leftrightarrow \quad C(\sum_{j\in J} P_j, G_1)/C(\sum_{j\in J} P_j, G_2) \simeq C(P_1 + \cdots + P_n, G_1)/C(P_1 + \cdots + P_n, G_2)\\
&\Leftrightarrow \quad \ker(P_J) \cap C(P_1 + \cdots + P_n, G_1) = \ker(P_J) \cap C(P_1 + \cdots + P_n, G_2)\\
&\Leftrightarrow \quad C(\sum_{j\notin J} P_J, G_1 - \sum_{j\in J} P_j) = C(\sum_{j\notin J} P_J, G_2 - \sum_{j\in J} P_j)\\
&\Leftrightarrow \quad f_1 \in \mathscr{L}(G_1 - \sum_{j\in J} P_j) \Rightarrow \exists f_2 \in \mathscr{L}(G_2 - \sum_{j\in J} P_j) \text{ s.t. } f_1(P_j) = f_2(P_j) \forall j \notin J\\
&\Leftrightarrow \quad f_1 \in \mathscr{L}(G_1 - \sum_{j\in J} P_j) \Rightarrow \exists f_2 \in \mathscr{L}(G_2 - \sum_{j\in J} P_j) \text{ s.t. } f_1 - f_2 \in \mathscr{L}(G_1 - \sum_{j\notin J} P_j)\\
&\Leftrightarrow \quad \forall f_1 \in \mathscr{L}(G_1 - \sum_{j\in J} P_j), \exists f_2 \in \mathscr{L}(G_2 - \sum_{j\in J} P_j), \exists f_3 \in \mathscr{L}(G_1 - \sum_{j=1}^{n} P_j) \text{ s.t. } f_1 = f_2 + f_3\\
&\Leftrightarrow \quad \mathscr{L}(G_1 - \sum_{j\in J} P_j) \subseteq \mathscr{L}(G_1 - \sum_{j=1}^{n} P_j) + \mathscr{L}(G_2 - \sum_{j\in J} P_j)
\end{aligned}$$

$$
\begin{aligned}
&\Leftrightarrow\quad v_Q(\mathscr{L}(G_1-\sum_{j\in J}P_j))\subseteq v_Q(\mathscr{L}(G_1-\sum_{j=1}^{n}P_j)+\mathscr{L}(G_2-\sum_{j\in J}P_j))\\
&\Leftarrow\quad v_Q(\mathscr{L}(G_1-\sum_{j\in J}P_j))\subseteq v_Q(\mathscr{L}(G_1-\sum_{j=1}^{n}P_j))\cup v_Q(\mathscr{L}(G_2-\sum_{j\in J}P_j)). \qquad (7)
\end{aligned}
$$

For any rational place Q and any divisor G of F, $v_Q(\mathscr{L}(G))$ can be computed by **Gröbner bases** and the algorithm in [11], provided that the defining equations of F is in special position with respect to Q [6, 8, 12].

We turn our attention to (2). Equation (2) holds

$$
\begin{aligned}
&\Leftrightarrow\quad C(\sum_{j\in J}P_j,G_1)=C(\sum_{j\in J}P_j,G_2)\\
&\Leftrightarrow\quad \forall f_1\in\mathscr{L}(G_1),\exists f_2\in\mathscr{L}(G_2)\text{ s.t. } f_1-f_2\in\mathscr{L}(-\sum_{j\in J}P_j+G_1)\\
&\Leftrightarrow\quad \forall f_1\in\mathscr{L}(G_1),\exists f_2\in\mathscr{L}(G_2),\exists f_3\in\mathscr{L}(-\sum_{j\in J}P_j+G_1)\text{ s.t. } f_1=f_2+f_3\\
&\Leftrightarrow\quad \mathscr{L}(G_1)=\mathscr{L}(G_2)+\mathscr{L}(G_1-\sum_{j\in J}P_j)\\
&\Leftrightarrow\quad v_Q(\mathscr{L}(G_1))=v_Q(\mathscr{L}(G_2)+\mathscr{L}(G_1-\sum_{j\in J}P_j))\\
&\Leftarrow\quad v_Q(\mathscr{L}(G_1))=v_Q(\mathscr{L}(G_2))\cup v_Q(\mathscr{L}(G_1-\sum_{j\in J}P_j)). \qquad (8)
\end{aligned}
$$

A similar sufficient condition for (3) can be deduced from (4) and (5).

2.2 Explicit Sufficient Conditions

We explicitly write sufficient conditions for (7) and (8), and examine if they are easier to hold than (4) and (5) for one point AG codes with $G_1 = m_1Q$ and $G_2 = m_2Q$. For any divisor G, let $H_Q(G) = -v_Q(\mathscr{L}(G+\infty Q)\setminus\{0\})$. Observe that $H_Q(0)$ is the Weierstrass semigroup at Q. The conductor of $H_Q(G)$ is defined as $\min\{i\in H_Q(G)\mid i\le j\in\mathbf{N}\Rightarrow j\in H_Q(G)\}$, which generalizes the conductor of the Weierstrass semigroup $H_Q(0)$.

Equation (7) holds if

$$
\begin{aligned}
&v_Q(\mathscr{L}(m_1Q-\sum_{j\in J}P_j)\setminus\{0\})=\emptyset\\
\Leftrightarrow\quad &m_1\le \min H_Q(-\sum_{j\in J}P_j)-1 \qquad (9)
\end{aligned}
$$

We see that condition (9) is less demanding than (4), because $\min H_Q(-\sum_{j\in J}P_j)\ge |J|$.

Similarly, (8) holds if

$$
m_2\ge \text{the conductor of } H_Q(-\sum_{j\in J}P_j)-1 \qquad (10)
$$

We also see that condition (10) is less demanding than (5), because the conductor of $H_Q(-\sum_{j\in J} P_j)$ is $\leq 2g(F)$. We can also make a similar improvement over (6): Condition (6) holds if

$$m_1 \leq \min H_Q(-\sum_{j\in J} P_j) - 1 \text{ and } m_2 \geq \text{the conductor of } H_Q(-\sum_{j\notin J} P_j) - 1.$$

In particular, for elliptic function fields ($g(F) = 1$),

$$(9) \quad \Leftrightarrow \quad \begin{cases} m_1 + 1 \leq |J| & \text{if } \exists f \in \mathscr{L}(\infty Q), (f)_0 = \sum_{j\in J} P_j, \\ m_1 \leq |J| & \text{otherwise} \end{cases} \tag{11}$$

$$(10) \quad \Leftrightarrow \quad \begin{cases} |J| \leq m_2 - 1 & \text{if } \exists f \in \mathscr{L}(\infty Q), (f)_0 = \sum_{j\in J} P_j, \\ |J| \leq m_2 & \text{otherwise} \end{cases} \tag{12}$$

Acknowledgment

The authors gratefully acknowledge the support from Japan Society for the Promotion of Science (Grant Nos. 23246071 and 26289116), from the Spanish MINECO (Grant No. MTM2012-36917-C03-03), the Danish Council for Independent Research (Grant No. DFF-4002-00367) and from the “Program for Promoting the Enhancement of Research Universities” at Tokyo Institute of Technology.

References

[1] T. Bains. Generalized Hamming weights and their applications to secret sharing schemes. Master’s thesis, University of Amsterdam, Feb. 2008. supervised by R. Cramer, G. van der Geer, and R. de Haan.

[2] G. R. Blakley and C. Meadows. Security of ramp schemes. In *Advances in Cryptology–CRYPTO’84*, volume 196 of *Lecture Notes in Computer Science*, pages 242–269. Springer-Verlag, 1985. doi:10.1007/3-540-39568-7_20.

[3] H. Chen, R. Cramer, R. de Haan, and I. Cascudo Pueyo. Strongly multiplicative ramp schemes from high degree rational points on curves. In N. Smart, editor, *Advances in Cryptology – EUROCRYPT 2008*, volume 4965 of *Lecture Notes in Computer Science*, pages 451–470. Springer-Verlag, 2008. doi:10.1007/978-3-540-78967-3_26.

[4] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan. Secure computation from random error correccting codes. In *Advances in Cryptology–EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Computer Science*, pages 291–310. Springer-Verlag, 2007. doi:10.1007/978-3-540-72540-4_17.

[5] R. Cleve, D. Gottesman, and H.-K. Lo. How to share a quantum secret. *Phys. Rev. Lett.*, 83(3):648–651, July 1999. quant-ph/9901025, doi:10.1103/PhysRevLett.83.648.

[6] O. Geil and R. Pellikaan. On the structure of order domains. *Finite Fields and Their Appl.*, 8:369–396, 2002.

[7] D. Gottesman. Theory of quantum secret sharing. *Phys. Rev. A*, 61(4), Mar. 2000. quant-ph/9910067, doi:10.1103/PhysRevA.61.042311.

[8] C. Heegard, J. Little, and K. Saints. Systematic encoding via Gröbner bases for a class of algebraic-geometric Goppa codes. *IEEE Trans. Inform. Theory*, 41(6):1752–1761, Nov. 1995.

[9] J. Kurihara, T. Uyematsu, and R. Matsumoto. Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight. *IEICE Trans. Fundamentals*, E95-A(11):2067–2075, Nov. 2012. doi:10.1587/transfun.E95.A.2067.

[10] R. Matsumoto. Coding theoretic construction of quantum ramp secret sharing. (version 4 or later), May 2014. arXiv:1405.0149v5.

[11] R. Matsumoto and S. Miura. Finding a basis of a linear system with pairwise distinct discrete valuations on an algebraic curve. *J. Symbolic Comput.*, 30(3):309–323, Sept. 2000. doi:10.1006/jsco.2000.0372.

[12] R. Matsumoto and S. Miura. On construction and generalization of algebraic geometry codes. In T. Katsura et al., editors, *Proc. Algebraic Geometry, Number Theory, Coding Theory, and Cryptography*, pages 3–15, Univ. Tokyo, Japan, Jan. 2000. Available from: http://www.rmatsumoto.org/repository/weight-construct.pdf.

[13] W. Ogata, K. Kurosawa, and S. Tsujii. Nonperfect secret sharing schemes. In *Advances in Cryptology – AUSCRYPT '92*, volume 718 of *Lecture Notes in Computer Science*, pages 56–66. Springer-Verlag, 1993. doi:10.1007/3-540-57220-1_52.

[14] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto. Quantum secret sharing schemes and reversibility of quantum operations. *Phys. Rev. A*, 72(3), Sept. 2005. quant-ph/0505001, doi:10.1103/PhysRevA.72.032318.

[15] A. Shamir. How to share a secret. *Comm. ACM*, 22(11):612–613, Nov. 1979. doi:10.1145/359168.359176.

[16] A. D. Smith. Quantum secret sharing for general access structures. Jan. 2000. quant-ph/0001087.

[17] H. Yamamoto. Secret sharing system using (k, l, n) threshold scheme. *Electronics and Communications in Japan (Part I: Communications)*, 69(9):46–54, 1986. (the original Japanese version published in 1985). doi:10.1002/ecja.4410690906.

[18] P. Zhang and R. Matsumoto. Quantum strongly secure ramp secret sharing. *Quantum Information Processing*, 14(2):715–729, Feb. 2015. doi:10.1007/s11128-014-0863-2.

Quantum codes with bounded minimum distance

Carlos Galindo[1] , Fernando Hernando[2], Diego Ruano[3]

[1] *Universidad Jaume I, Spain, galindo@mat.uji.es*
[2] *Universidad Jaume I, Spain, carrillf@uji.es*
[3] *Aalborg University, Denmark, diego@math.aau.dk*

Polynomial time algorithms for prime factorization and discrete logarithms on quantum computers were given by Shor in 1994 [14]. Thus, if an efficient quantum computer existed (see [2, 17], for recent advances), most popular cryptographic systems could be broken and much computational work could be done much faster. Unlike classical information, quantum information cannot be cloned [5, 20], despite this fact quantum (error-correcting) codes do exist [15, 18]. The above facts explain why, in the last decades, the interest in quantum computations and, in particular, in quantum coding theory grew dramatically.

Set $q = p^r$ a positive power of a prime number p, and let $\mathbb{C}^q$ be a q-dimensional complex vector space. A $((n,K,d))_q$ quantum error correcting code is a q-ary subspace Q of $\mathbb{C}^{q^n} = \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q$ with dimension K and minimum distance d. If $K = q^k$ we will write $[[n,k,d]]_q$.

Constructing and computing the paramters of a quantum code is in general a difficult task. In [3] Calderbank et al stablish the basis to use classical linear codes (either with the Hermitian or the Euclidean inner product) to construct a class of quantum codes named stabilizer codes. Later their results were generalized for an arbitrary finite field [13, 1]. Most of the codes known so far are obtined via the following result.

Theorem 1. *[13, 1] The following two statements hold.*

1. *Let C be a linear $[n,k,d]$ error-correcting code over $\mathbb{F}_q$ such that $C^\perp \subseteq C$. Then, there exists an $[[n,2k-n,\geq d]]_q$ stabilizer code which is pure to d. If the minimum distance of $C^\perp$ exceeds d, then the stabilizer code is pure and has minimum distance d.*

2. *Let C be a linear $[n,k,d]$ error-correcting code over $\mathbb{F}_{q^2}$ such that $C^{\perp_h} \subseteq C$. Then, there exists an $[[n,2k-n,\geq d]]_q$ stabilizer code which is pure to d. If the minimum distance $d^{\perp_h}$ of the code $C^{\perp_h}$ exceeds d, then the stabilizer code is pure and has minimum distance d.*

Codes obtained as described in Item (1) of Theorem 1 are usually referred to as obtained from the CSS construction [4, 18]. The parameters of the codes coming from Item (1) of Theorem 1 can be improved with the Hamada's generalization

[12] of the Steane's enlargement procedure [19]. Let us state the result, where wt denotes minimum weight.

Theorem 2. *[12] Let C be an $[n,k]$ linear code over the field $\mathbb{F}_q$ such that $C^\perp \subseteq C$. Assume that C can be enlarged to an $[n,k']$ linear code C', where $k' \geq k+2$. Then, there exists a stabilizer code with parameters $[[n,k+k'-n,d \geq \min\{d', \lceil \frac{q+1}{q} d\text{"} \rceil\}]]_q$, where $d' = \mathrm{wt}(C \setminus C'^\perp)$ and $d\text{"} = \mathrm{wt}(C' \setminus C'^\perp)$.*

We propose to work with the so called family of J-affine variety codes and characterize when a code within this family is contained in its dual (either Hermitian or Euclidean), see [6, 7, 8] for more details.

Consider the ring of polynomials $\mathbb{F}_q[X_1,X_2,\ldots,X_m]$ in m variables over the field $\mathbb{F}_q$ and fix m integers $N_j > 1$ such that $N_j - 1$ divides $q-1$ for $1 \leq j \leq m$. For a subset $J \subseteq \{1,2,\ldots,m\}$, set I_J the ideal of the ring $\mathbb{F}_q[X_1,X_2,\ldots,X_m]$ generated by $X_j^{N_j} - X_j$ whenever $j \notin J$ and by $X_j^{N_j-1} - 1$ otherwise, for $1 \leq j \leq m$. We denote by R_J the quotient ring $\mathbb{F}_q[X_1,X_2,\ldots,X_m]/I_J$.

Set $Z_J = Z(I_J) = \{P_1,P_2,\ldots,P_{n_J}\}$ the set of zeros over $\mathbb{F}_q$ of the defining ideal of R_J. Clearly, the points P_i, $1 \leq i \leq n_J$, can have 0 as a coordinate for those indices j which are not in J but this is not the case for the remaining coordinates. Denote by $\mathrm{ev}_J : R_J \to \mathbb{F}_q^{n_J}$ the evaluation map defined as $\mathrm{ev}_J(f) = (f(P_1), f(P_2), \ldots, f(P_{n_J}))$, where $n_J = \prod_{j \notin J} N_j \prod_{j \in J}(N_j - 1)$. Set $T_j = N_j - 1$ except when $j \in J$, in this last case, $T_j = N_j - 2$, consider the set

$$\mathscr{H}_J := \{0,1,\ldots,T_1\} \times \{0,1,\ldots,T_2\} \times \cdots \times \{0,1,\ldots,T_m\}$$

and a nonempty subset $\Delta \subseteq \mathscr{H}_J$. Then, we define the J-affine variety code given by Δ, E_Δ^J, as the vector subspace (over $\mathbb{F}_q$) of $\mathbb{F}_q^{n_J}$ generated by the evaluation by ev_J of the set of classes in R_J corresponding to monomials $X^a := X_1^{a_1} X_1^{a_2} \cdots X_m^{a_m}$ such that $a = (a_1,a_2,\ldots,a_m) \in \Delta$. Stabilizer codes constructed from $\{1,2,\ldots,m\}$-affine variety codes were considered in [6, 7] because they allowed us to do comparisons with some quantum BCH codes. What we call $\emptyset$-affine variety codes are simply called affine variety codes in [9]. We will stand $\mathscr{H}$ for $\mathscr{H}_\emptyset$. Notice that considering different sets J we get codes of different lengths

$$(N_1 - 1)(N_2 - 1) \cdots (N_m - 1) = n_{\{1,2,\ldots,m\}} \leq n_J \leq n_\emptyset = N_1 N_2 \cdots N_m.$$

We provide a generalization of the bound given in [10]. We define $\varepsilon_i = 1$ if $i \in J$ and 0 otherwise.

Proposition 1. *Let $p(X) \in \mathbb{F}_q[X_1,X_2,\ldots,X_m]$ (we may also think that is a reduced class on R), with leading monomial $X^a := X_1^{a_1} X_1^{a_2} \cdots X_m^{a_m}$ where $a_i \leq T_i$ for $i = 1,\ldots,m$ then the number of points in $Z(I)$ which are not a root of $p(X)$ is:*

$$\delta_a \geq \prod_{j=1}^{m}(N_j - a_j - \varepsilon_j).$$

The minimum distance of the quantum code induced by Δ is bounded by the minimum distance of the dual $E_\Delta^\perp = E_{\Delta^\perp}$. In terms of the previous lower bound

$$d(E_{\Delta^\perp}) \geq min\{\delta_a \mid a \in \Delta^\perp\}. \tag{1}$$

Hyperbolic-like codes are constructed ad hoc in order to maximize the lower bound (1). Hyperbolic codes were studied in [11] in the particular case were $N_1 = \cdots = N_m = q^r$ and $J = \emptyset$. We propose the following generalization in this work.

Let $n_J = \prod_{i=1}^{m}(T_i + 1)$ be the length of the code (or the size of $Z(I_J)$). Fix a positive integer t, $0 \leq t \leq n_J$, define the linear code $Hyp(t,m)$, over $F_q^{n_J}$, as the image of the evaluation map of the set of monomials:

$$M_m^J(t) = \left\{ x_1^{a_1} \cdots x_m^{a_m} : 0 \leq a_i \leq T_i, 1 \leq i \leq m, \prod_{i=1}^{m}(N_i - a_i - \varepsilon_i) \geq t \right\}$$

By definition and (1) the following result is clear.

Proposition 2. *The minimum weight, d, of $Hyp(t,m)$ satisfies $d \geq t$.*

With this definition we maximize the dimension of a code with lower bound greater than or equal to t.

Next question is to determine its dual. We define the linear code $E(t)$, over $F_q^{n_J}$ as the image of the evaluation map of the set of monomials:

$$N_m^J(t) = \left\{ x_1^{b_1} \cdots x_m^{b_m} : \varepsilon_i \leq b_i \leq T_i, 1 \leq i \leq m, \prod_{i=1}^{m}(b_i + 1 - \varepsilon_i) < t \right\}$$

Proposition 3. *Let us assume that there exists $j \notin J$ such that $p \mid N_j$. Then $E(t)^\perp = Hyp(t,m)$ (where $\perp$ denotes the euclidean dual).*

Theorem 3. *Let $q = p^r$ and $N_1 - 1, N_2 - 1 \mid q^2 - 1$ and assume that exists $j \notin J$ such that $p \mid N_j$. If any of the following cases hold:*

(i) $J = \emptyset$ and $p \mid N_j$ for all $j \notin J$ and exists i with $N_i - 1 \mid q - 1$, and $N_i - 1 > t - 3$ if t i odd and $N_i - 1 > t - 4$ if t is even.

(i') $J = \emptyset$ and exist i such that $N_i - 1 \mid q - 1$ and $N_i - 1 \geq 2(t-2) + 1$.

(ii) $J = \{1\}$ and $N_2 - 1 \mid q - 1$ and $N_2 - 1 \geq 2(t-2) + 1$.

(iii) $J=\{1\}$ *and* $N_1-1 \mid q-1$ *and* $N_1-1\geq t$ *if* t *odd and* $N_1-1\geq t-1$ *if* t *even.*

(iv) $J=\{1,2\}$ *and exists* i *such that* $N_i-1 \mid q-1$ *and* $N_i-1\geq 2(t-1)+1$.

Then there exist a quantum codes with parameters: $[[n_J, \geq n_J-2\#E(t), \geq t]]_q$.

Theorem 4. *Let* $q=p^r$ *and* $N_1-1, N_2-1 \mid q^2-1$ *and assume that exists* $j\notin J$ *such that* $p|\,N_j$. *If any of the following cases hold:*

(i) $J=\emptyset$ *and* $p|\,N_j$ *for all* $j\notin J$ *and exists* i *such that* $N_i-1 \mid q^2-1$ *and* $N_i-1 > (\frac{t-1}{2}-1)(q+1)$ *if* t *is odd and* $N_i-1>(\frac{t}{2}-1)(q+1)$ *if* t *is even.*

(i') $J=\emptyset$ *and exist* i *such that* $N_i-1 \mid q^2-1$ *and* $N_i-1>(t-2)(q+1)\geq (t-2)(q+1)+1$.

(ii) $J=\{1\}$ *and* $N_2-1 \mid q^2-1$ *and* $N_2-1>(t-2)(q+1)\geq(t-2)(q+1)+1$.

(iii) $J=\{1\}$ *and* $N_1-1 \mid q^2-1$ *and* $N_1-1>(\frac{t-1}{2})(q+1)$ *if* t *is odd and* $N_1-1>(\frac{t}{2}-1)(q+1)$ *if* t *is even.*

(iv) $J=\{1,2\}$ *and exist* i *such that* $N_i-1 \mid q^2-1$ *and* $N_i-1>(q+1)(t-1)$.

Then there exist a quantum code with parameters $[[n_J, \geq n_J-2\#E(t), \geq t]]_q$.

Furthermore, we present the following generalization of the Steane's enlargement procedure that allowed us to obtain excellent codes in [8].

Theorem 5. *Let* C_1 *and* $\hat{C}_1$ *be two linear codes over the field* $\mathbb{F}_q$, *with parameters* $[n,k_1,d_1]$ *and* $[n,\hat{k}_1,\hat{d}_1]$ *respectively, and such that* $C_1^{\perp}\subseteq\hat{C}_1$. *Consider a linear code* $D\subseteq\mathbb{F}_q^n$ *such that* $\dim D\geq 2$ *and* $(C_1+\hat{C}_1)\cap D=\{0\}$. *Set* $C_2=C_1+D$ *and* $\hat{C}_2=C_2+D$, *that enlarge* C_1 *and* $\hat{C}_1$ *respectively, with parameters* $[n,k_2,d_2]$ *and* $[n,\hat{k}_2,\hat{d}_2]$ *(*$k_2-k_1=\hat{k}_2-\hat{k_1}=\dim D>1$*). Set* C_3 *the code sum of the vector spaces* $C_1+\hat{C}_1+D$, *whose parameters we denote by* $[n,k_3,d_3]$. *Then, there exists a stabilizer code with parameters*

$$\left[\left[n, k_2+\hat{k}_1-n, d\geq \min\left\{d_1,\hat{d}_1,\left\lceil\frac{d_2+\hat{d}_2+d_3}{2}\right\rceil\right\}\right]\right]_2,$$

when $q=2$. *Otherwise, the parameters are*

$$\left[\left[n,k_2+\hat{k}_1-n,d\geq\min\left\{d_1,\hat{d}_1,M\right\}\right]\right]_q,$$

where $M=\max\{d_3+\lceil(d_2/q)\rceil, d_3+\lceil(\hat{d}_2/q)\rceil\}$.

Acknowledgment: The authors gratefully acknowledge the support from the Spanish MINECO (Grant No. MTM2012-36917-C03-03), the Danish Council for Independent Research (Grant No. DFF-4002-00367) and from the "Program for Promoting the Enhancement of Research Universities" at Tokyo Institute of Technology.

References

[1] Aly, S.A., Klappenecker, A., Kumar, S., Sarvepalli, P.K. On quantum and classical BCH codes, *IEEE Trans. Inf. Theory* **53** (2007) 1183-1188.

[2] Bian, Z. et al. Experimental determination of Ramsey numbers, *Phys. Rev. Lett.* **111** 130505 (2013).

[3] Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A. Quantum error correction via codes over GF(4), *IEEE Trans. Inf. Theory* **44** (1998) 1369-1387.

[4] Calderbank A.R., Shor, P. Good quantum error-correcting codes exist, *Phys. Rev. A* **54** (1996) 1098-1105.

[5] Dieks, D. Communication by EPR devices, *Phys. Rev. A* **92** (1982) 271.

[6] Galindo, C., Hernando, F. Quantum codes from affine variety codes and their subfield subcodes. To appear in *Des. Codes Crytogr.*

[7] Galindo, C., Hernando, F., Ruano, D. New quantum codes from evaluation and matrix-product codes. Preprint arXiv:1406.0650.

[8] Galindo, C., Hernando, F., Ruano, D. Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement . Preprint arXiv:1503.00879. To appear in *Quantum Inf. Process.*

[9] Geil, O. *Evaluation codes from an affine variety code perspective*. Advances in algebraic geometry codes, Ser. Coding Theory Cryptol. 5 (2008) 153-180. World Sci. Publ., Hackensack, NJ. Eds.: E. Martinez-Moro, C. Munuera, D. Ruano.

[10] Geil, O. Roots and coefficients of multivariate polynomials over finite fields, to appear in Finite Fields and their applications.

[11] Geil, O., Høholdt, T. On hyperbolic codes, *Lect. Notes Comp. Sc.* **2227** (2001) 159-171.

[12] Hamada, M. Concatenated quantum codes constructible in polynomial time: Efficient decoding and error correction, *IEEE Trans. Inform. Theory* **54** (2008) 5689-5704.

[13] Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.K. Nonbinary stabilizer codes over finite fields, *IEEE Trans. Inform. Theory* **52** (2006) 4892-4914.

[14] Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, in Proc. 35th ann. symp. found. comp. sc., *IEEE Comp. Soc. Press* 1994, 124-134.

[15] Shor, P.W. Scheme for reducing decoherence in quantum computer memory, *Phys. Rev. A* **52** (1995) 2493-2496.

[16] Shor, P.W., Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol, *Phys. Rev. Lett.* **85** (2000) 441-444.

[17] Smith, G., Smolin, J. Putting “quantumness" to the test, *Physics* **6** 105 (2013).

[18] Steane, A.M. Simple quantum error correcting codes, *Phys. Rev. Lett.* **77** (1996) 793-797.

[19] Steane, A.M. Enlargement of Calderbank-Shor-Steane quantum codes, *IEEE Trans. Inform. Theory* **45** (1999) 2492-2495.

[20] Wootters W.K., Zurek, W.H. A single quantum cannot be cloned, *Nature* **299** (1982) 802-803.

Refined analysis of RGHWs of code pairs coming from Garcia-Stichtenoth's second tower

O. Geil[1], S. Martin[1], U. Martínez-Peñas[1], D. Ruano[1]

[1] *Aalborg University, Aalborg, Denmark, {olav,stefano,umberto,diego}@math.aau.dk*

1 Introduction

Relative generalized Hamming weights (RGHW) of two linear codes are fundamental for evaluating the security of ramp secret sharing schemes and wire-tap channels of type II [3, 4]. Until few years ago only for MDS codes and a few other examples of codes the hierarchy of the RGHWs was known [6], but recently new results were discovered for one-point algebraic geometric codes [3], q-ary Reed-Muller codes [7] and cyclic codes [8]. In [2] it was discussed how to obtain asymptotically good sequences of ramp secret sharing schemes by using one-point algebraic geometric codes defined from good towers of function fields. The tools used here were the Goppa bound and the Feng-Rao bounds. In the present paper we focus on secret sharing schemes coming from the Garcia-Stichtenoth second tower [1]. We demonstrate how to obtain refined information on the RGHW's when the codimension is small. For general co-dimension we give an improved estimate on the highest RGHW. The new results are obtained by studying in detail the sequence of Weierstrass semigroups related to a sequence of rational places [5].

We recall the definition of RGHWs and briefly mention their use in connection with secret sharing schemes.

Definition 1 *Let $C_2 \subsetneq C_1$ be two linear codes. For $m = 1,\dots,\dim C_1 - \dim C_2$ the m-th relative generalized Hamming weight (RGHW) of C_1 with respect to C_2 is*

$$M_m(C_1,C_2) = \min\{\#\mathrm{Supp} D \mid D \subseteq C_1 \textit{ is a linear space,}$$
$$\dim D = m, D\cap C_2 = \{\vec{0}\}\}. \quad (1)$$

Here $\mathrm{Supp} D = \#\{i \in \mathbb{N} \mid$ *exists* $(c_1,\dots,c_n) \in D$ *with* $c_i \neq 0\}$.
For $m = 1,\dots,\dim C_1$ the m-th generalized Hamming weight (GHW) $d_m(C_1)$ is equal to $M_m(C_1,\{\vec{0}\})$.

It was proved in [3, 4] that a secret sharing secret scheme obtained from two linear codes $C_2 \subsetneq C_1$ has $r_m = n - M_{\ell-m+1}(C_1,C_2) + 1$ reconstruction and $t_m = M_m(C_2^\perp, C_1^\perp) - 1$ privacy for $m = 1,\dots,\ell$. Here, r_m and t_m are the unique numbers such that the following holds: It is not possible to recover m q-bits of information about the secret with only t_m shares, but it is possible with some $t_m + 1$ shares. With any r_m shares it is possible to recover m q-bits of information about the secret, but it is not possible to recover m q-bits of information with some $r_m - 1$ shares.

We shall focus on one-point algebraic geometric codes $C_{\mathscr{L}}(D,G)$ where $D = P_1 + \cdots + P_n$, $G = \mu Q$, and $P_1, \ldots, P_n, Q$ are pairwise different rational places over a function field. By writing v_Q for the valuation at Q, the Weierstrass semigroup corresponding to Q is

$$H(Q) = -v_Q \left(\bigcup_{\mu=0}^{\infty} \mathscr{L}(\mu Q) \right) = \{\mu \in \mathbb{N}_0 \mid \mathscr{L}(\mu Q) \neq \mathscr{L}((\mu-1)Q)\}. \quad (2)$$

We denote by g the genus of the function field and by c the conductor of the Weierstrass semigroup.

We consider $C_1 = C_{\mathscr{L}}(D, \mu_1 Q)$ and $C_2 = C_{\mathscr{L}}(D, \mu_2 Q)$, with $-1 \leq \mu_2 < \mu_1$. Observe that for $\ell = \dim(C_1) - \dim(C_2)$ and $\mu = \mu_1 - \mu_2$ we have that $\ell \leq \mu$, with equality if $2g \leq \mu_2 < \mu_1 \leq n-1$ holds.

From [2, Proposition 23 and its proof] we have the following result:

Proposition 2 *If* $1 \leq m \leq \min\{\ell, c\}$*, then*

$$M_m(C_1, C_2) \geq n - \mu_1 + (m-1) + (m - c + g + h_{c-m}) \quad (3)$$

where $h_{c-m} = \#(H(Q) \cap (0, c-m])$. *If* $2g \leq \mu_1 \leq n-1$*, then*

$$M_m(C_1, C_2) \geq n - \dim C_1 + 2m - c + h_{c-m} \quad (4)$$

Applying Proposition 2 to code pairs coming from Garcia-Sticthenoth's second tower [1] the following asymptotically result was obtained in [2, Corollary 40]:

Corollary 3 *Let q be an even power of a prime and* $0 \leq \rho \leq \frac{1}{\sqrt{q}-1}$. *There exists a sequence of one-point algebraic geometric codes* $C_i = C_{\mathscr{L}}(D, \mu_i Q)$ *and a sequence of positive integers m_i such that for i going to infinity:* $n_i = n(C_i) \to \infty$, $\dim C_i / n_i \to R$, $\mu_i / n_i \to \tilde{R}$, $m_i / n_i \to \rho$. *Let* $\delta = \liminf d_{m_i}(C_i)/n_i$, *we have that:*

$$\delta \geq 1 - \tilde{R} + 2\rho. \quad (5)$$

If $\frac{1}{\sqrt{q}-1} \leq R \leq 1$, *we have that:*

$$\delta \geq 1 - R + 2\rho - \frac{1}{\sqrt{q}-1}. \quad (6)$$

From Garcia-Stichtenoth's second tower [1] one obtains codes over any field $\mathbb{F}_q$ where q is an even power of a prime. Garcia and Stichtenoth analyzed the asymptotic behavior of the number of rational places and the genus, from which it is clear that the codes beat the Gilbert-Varshamov bound for $q \geq 49$. Remarkably, a complete description of the Weierstrass semigroups corresponding to a sequence of rational places was given in [5]. This description is what allows us to refine in the present paper the analysis of the RGHWs.

2 Small codimension

In this section we give a sharper bound on the RGHWs of two one-point algebraic geometric codes coming from Stichtenoth-Garcia's towers when the codimension is small.

Proposition 4 *Let ν be an even positive integer and q an even power of a prime. Consider two one-point algebraic geometric codes $C_2 \subsetneq C_1$ defined from the ν-th Garcia-Stichtenoth function field over $\mathbb{F}_q$. For $\mu < q^{\frac{\nu+1}{2}}$ and $m = 1, \ldots, \mu$, we have that:*

$$M_m(C_1,C_2) \geq n - \mu_1 + \min\left\{ (m-1)q^{\frac{\nu}{4}-\frac{1}{2}u} + \left\lfloor q^{u-\frac{1}{2}}\left(1-q^{-\frac{1}{2}}\right)\right\rfloor : \right.$$
$$\left. u \in \left\{ \left\lceil \log_q(m-1)+\frac{1}{2}\right\rceil, \left\lfloor \log_q(\mu-1)+\frac{1}{2}\right\rfloor \right\} \right\}. \tag{7}$$

Note that there are some cases where the minimum is reached for $u = \lceil \log_q(m-1)+\frac{1}{2}\rceil$ and other cases where it is reached for $u = \lfloor \log_q(\mu-1)+\frac{1}{2}\rfloor$. For this reason in Proposition 4 the value u is not univocal.

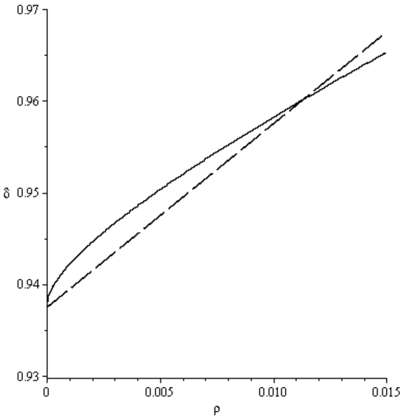
As Proposition 2, this result has an asymptotic implication:

Corollary 5 *Let q be an even power of a prime, $0 \leq \tilde{R}_2 \leq \tilde{R}_1 < 1$, and $\tilde{R} = \tilde{R}_1 - \tilde{R}_2 < \frac{1}{\sqrt{q}-1}$. There exists a sequence of pairs of one-point AG codes $C_{2,i} = C_{\mathscr{L}}(D_i, \mu_{2,i}Q) \subsetneq C_{1,i} = C_{\mathscr{L}}(D_i, \mu_{1,i}Q)$, such that: $n_i = n(C_{2,i}) = n(C_{1,i}) \to \infty$, $\mu_{j,i}/n_i \to \tilde{R}_j$ for $j = 1,2$ for $i \to \infty$. For a given ρ let m_i be such that $m_i/n_i \to \rho$ for $i \to \infty$ and let $M = \liminf M_{m_i}(C_{1,i},C_{2,i})/n_i$. The sequence of code pairs satisfies:*

$$M \geq 1 - \tilde{R}_1 + \min_{u \in \{\rho,\tilde{R}\}} \left\{ \rho\left(u(q-\sqrt{q})\right)^{-\frac{1}{2}} + \frac{u}{q}(q-\sqrt{q}) \right\}. \tag{8}$$

Note that if we assume that $C_{2,i}$ are zero codes for all i, then $\lim M_{m_i}(C_{1,i},\{\vec{0}\})$ is the asymptotically value of the m_i-th general Hamming weight of $C_{i,1}$. For $\tilde{R} < \frac{1}{4(q-\sqrt{q})}$, the bound in Corollary 5 is sharper than the one obtained in Corollary 3.

In the following graph we compare the bound from Corollary 3 (the dashed curve) with the bound from Corollary 5 (the solid curve). The first axis represents $\rho = \lim m_i/n_i$, and the second axis represents $\delta = \lim\inf M_{m_i}(C_{1,i},\{\vec{0}\})$.



3 The highest RGHW

In this section for $2g \leq \mu_2 < \mu_1 < n-1$, we obtain a new bound for the highest RGHW of two one-point algebraic geometric codes obtained from Stichtenoth-Garcia's second tower.

Proposition 6 *Let ν be an even positive integer and $2g \leq \mu_2 < \mu_1 < n-1$. Consider two one-point algebraic geometric codes $C_2 \subsetneq C_1$ built on the ν-th Garcia-Stichtenoth tower. We have that:*

$$M_\ell(C_1,C_2) = n - \dim C_2 \quad \text{if } \ell \geq q^{\frac{\nu-1}{2}} \tag{9}$$

$$M_\ell(C_1,C_2) \geq n - \dim C_2 - \left(q^{\frac{\nu-1}{2}} \sum_{i=1}^{\lfloor \frac{\nu+1}{2} - \log_q(\ell) \rfloor - 1} (q^{1-\frac{i}{2}} - q^{-\frac{i}{2}}) + \right.$$
$$\left. +(q^{\frac{\nu+1}{2} - \lfloor \frac{\nu+1}{2} - \log_q(\ell) \rfloor} - \ell) q^{\frac{\lfloor \frac{\nu+1}{2} - \log_q(\ell) \rfloor}{2}} \right) \quad \text{if } \ell < q^{\frac{\nu-1}{2}} \tag{10}$$

For $\ell \geq q^{\frac{\nu-1}{2}}$, the Singleton bound is reached. For $\ell < q^{\frac{\nu-1}{2}}$ it is still an interesting bound because we are able to estimate h_{c-m}. This bound has an asymptotically implication as well:

Corollary 7 *Let q be an even power of a prime, $\frac{2}{\sqrt{q}-1} \leq \tilde{R}_2 \leq \tilde{R}_1 < 1$, and $\tilde{R} = \tilde{R}_1 - \tilde{R}_2$. There exists a sequence of one-point algebraic geometric codes $C_{2,i} = C_{\mathscr{L}}(D_i, \mu_{2,i}Q) \subsetneq C_{1,i} = C_{\mathscr{L}}(D_i, \mu_{1,i}Q)$, $\mu_i = \mu_{1,i} - \mu_{2,i}$, such that: $n_i = n(C_{2,i}) = n(C_{1,i}) \to \infty$, $\mu_{j,i}/n_i \to \tilde{R}_j$ for $j = 1,2$ for $i \to \infty$. Let $\ell_i = \dim C_{1,i} - \dim C_{2,i}$, $M = \liminf M_{\ell_i}(C_{1,i}, C_{2,i})/n_i$, $R_j = \lim \frac{\dim C_{i,j}}{n_i}$ for $j = 1,2$, and $R = R_1 - R_2$, we have that:*

$$M = 1 - R_2 \quad \textit{if} \quad R \geq \frac{1}{q-\sqrt{q}} \tag{11}$$

and

$$M \geq 1 - R_2 - \left(\frac{1}{q-\sqrt{q}} \left(\sum_{i=1}^{-\lfloor \log_q (R(1-\frac{1}{\sqrt{q}})) \rfloor - 1} (q^{1-\frac{i}{2}} - q^{-\frac{i}{2}}) + \right. \right.$$

$$\left. \left. + q^{1+\frac{1}{2}\lfloor \log_q (R(1-\frac{1}{\sqrt{q}})) \rfloor} \right) - Rq^{-\frac{1}{2}\lfloor \log_q (R(1-\frac{1}{\sqrt{q}})) \rfloor} \right) \quad \textit{if} \quad R < \frac{1}{q-\sqrt{q}}. \tag{12}$$

In Corollary 3, ρ is smaller than or equal to $\frac{1}{\sqrt{q}-1}$. If we assume $C_{2,i}$ to be the zero codes for all i, then the value M of Corollary 7 represents the asymptotically value of the highest generalized Hamming weight of $C_{i,1}$. By using Corollary 3 for $R = \frac{1}{\sqrt{q}-1}$ it is possible to obtain a similar value, but for the other values of R it is a new bound.

References

[1] Arnaldo Garcia and Henning Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *Journal of Number Theory*, 61(2):248–273, 1996.

[2] Olav Geil, Stefano Martin, Umberto Martínez-Peñas, Ryutaroh Matsumoto, and Diego Ruano. Asymptotically good ramp secret sharing schemes. *arXiv:1502.05507*, 2015.

[3] Olav Geil, Stefano Martin, Ryutaroh Matsumoto, Diego Ruano, and Yuan Luo. Relative generalized hamming weights of one-point algebraic geometric codes. *Information Theory, IEEE Transactions on*, 60(10):5938–5949, 2014.

[4] Jun Kurihara, Tomohiko Uyematsu, and Ryutaroh Matsumoto. Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized hamming weight. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 95(11):2067–2075, 2012.

[5] Ruud Pellikaan, Henning Stichtenoth, and Fernando Torres. Weierstrass semigroups in an asymptotically good tower of function fields. *Finite fields and their applications*, 4(4):381–392, 1998.

[6] Zihui Liu, Wende Chen, and Yuan Luo. The relative generalized Hamming weight of linear q-ary codes and their subcodes. *Designs, Codes and Cryptography*, 48(2):111–123, 2008.

[7] Stefano Martin and Olav Geil. Relative generalized hamming weights of q-ary reed-muller codes. *arXiv:1407.6185*, 2014.

[8] Jun Zhang and Kequin Feng. Relative generalized hamming weights of cyclic codes. *arXiv:1505.07277*, 2015.

A new approach to the key equation and to the Berlekamp-Massey algorithm

M. Bras-Amorós[1], M. E. O'Sullivan[2], M. Pujol[1]

[1] *Universitat Rovira i Virgili, Tarragona, Catalonia, Spain, {maria.bras,marta.pujol}@urv.cat*
[2] *San Diego State University, California, USA, mosulliv@sciences.sdsu.edu*

The two primary decoding algorithms for Reed-Solomon codes are the Berlekamp-Massey algorithm [5] and the Sugiyama et al. adaptation of the Euclidean algorithm [7], both designed to solve Berlekamp's key equation [1]. Their connections are analyzed in [2, 4, 6]. We present a new version of the key equation for errors and erasures, more natural somehow, and a way to use the Euclidean algorithm to solve it. A straightforward reorganization of the algorithm yields the Berlekamp-Massey algorithm.

Settings on Reed-Solomon codes Let $\mathbb{F}$ be a finite field of size q and let α be a primitive element in $\mathbb{F}$. Let $n=q-1$. We identify the vector $u=(u_0,\dots,u_{n-1})$ with the polynomial $u(x)=u_0+\cdots+u_{n-1}x^{n-1}$ and denote $u(a)$ the evaluation of $u(x)$ at a. Classically the (primal) Reed-Solomon code $C^*(k)$ of dimension k is defined as the cyclic code with generator polynomial $(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{n-k})$, The dual Reed-Solomon code $C(k)$ of dimension k is the cyclic code with generator polynomial $(x-\alpha^{n-(k+1)})(x-\alpha^{n-(k+2)})\cdots(x-\alpha)(x-1)$.

Both codes have minimum distance $d=n-k+1$. Furthermore, $C(k)^\perp = C^*(n-k)$. There is a natural bijection from $\mathbb{F}^n$ to itself which we denote by $c\mapsto c^*$. It takes $C(k)$ to $C^*(k)$. The codeword c^* can be defined either as $iG^*(k)\in C^*(k)$ where i is the information vector of dimension k such that $c=iG(k)\in C(k)$ or componentwise as $c^*=(c_0,\alpha^{-1}c_1,\alpha^{-2}c_2,\dots,\alpha c_{n-1})$ where $c=(c_0,c_1,\dots,c_{n-1})$. Then, $(c_0^*,\alpha c_1^*,\alpha^2c_2^*,\dots,\alpha^{n-1}c_{n-1}^*)$. In particular, $c(\alpha^i)=c^*(\alpha^{i+1})$.

A decoding algorithm for a primal Reed-Solomon code may be used to decode a dual Reed-Solomon code by first applying the bijection $*$ to the received vector u. If u differs from a codeword $c\in C(k)$ by an error vector e of weight t, then u^* differs from the codeword $c^*\in C^*(k)$ by the error vector e^* of weight t. If the primal Reed-Solomon decoding algorithm can decode u^* to obtain c^* and e^* then, transforming by the inverse of $*$ we may obtain c and e. Conversely, a decoding algorithm for a dual Reed-Solomon code may be used to decode a primal Reed-Solomon code by applying the inverse of $*$, decoding, and then applying $*$.

Decoding for errors and erasures Suppose that $c\in C(k)$ is transmitted and that errors occurred at t different positions and that other s positions were erased, with

$2t+s<d$. Suppose that u is the received word once the erased positions are put to 0 and that $e=u-c$. Define the *erasure locator polynomial* as $\Lambda_r = \prod_{i:c_i \text{was erased}}(x-\alpha^i)$ and the *error locator polynomial* as $\Lambda_e = \prod_{i:e_i\neq 0, c_i \text{not erased}}(x-\alpha^i)$. We will use Λ for the product $\Lambda_r\Lambda_e$. Notice that Λ_r is known from the received word, while Λ_e is not. Define the error evaluator as $\Omega = \sum_{\substack{i:e_i\neq 0\\ \text{or } c_i \text{ erased}}} e_i \prod_{\substack{j:e_j\neq 0 \text{ or } c_j \text{ erased,}\\ \text{and } j\neq i}}(x-\alpha^i)$. The error positions can be identified by $\Lambda_e(\alpha^i)=0$ and the error values, as well as the erased values, can be derived from an analogue of the Forney formula [3], $e_i = \frac{\Omega(\alpha^i)}{\Lambda'(\alpha^i)}$.

The *syndrome polynomial* is defined as $S = e(\alpha^{n-1}) + e(\alpha^{n-2})x + \cdots + e(\alpha)x^{n-2} + e(1)x^{n-1}$. It can be proved that $\Omega(x^n-1) = \Lambda S$.The general term of S is $e(\alpha^{n-1-i})x^i$, but from a received word we only know $e(1)=u(1),\ldots,e(\alpha^{n-k-1}) = u(\alpha^{n-k-1})$. Define $\bar{S} = e(\alpha^{n-k-1})x^k + e(\alpha^{n-k-2})x^{k+1} + \cdots + e(1)x^{n-1}$. The polynomial $\Omega(x^n-1) - \Lambda\bar{S} = \Lambda(S-\bar{S})$ has degree at most $t+s+k-1 < \frac{d-s}{2} + s + n - d = n - \frac{d-s}{2}$. Next theorem provides an alternative key equation for dual Reed-Solomon codes.

Theorem 1. *If s erasures and at most $\lfloor \frac{d-s-1}{2} \rfloor$ errors occurred, then Λ_e and Ω are the unique polynomials f and φ satisfying the following properties. 1. $deg(f\Lambda_r\bar{S} - \varphi(x^n-1)) < n - \frac{d-s}{2}$; 2. $deg(f) \leq \frac{d-s}{2}$; 3. f,φ are coprime; 4. f is monic*

Suppose first that only erasures occurred. Then $\Lambda = \Lambda_r$, $\Lambda_e = 1$, and Ω can be directly derived from this inequality. Indeed, Ω is the sum of monomials in $\Lambda_r\bar{S}$ with degrees at least $n-\frac{d-s}{2}$, divided by $x^{n-\frac{d-s}{2}}$.

Suppose that a combination of errors and erasures occured. The extended Euclidean algorithm applied to $\Lambda_r\bar{S}$ and $-(x^n-1)$ computes not only $\gcd(\Lambda_r\bar{S}, x^n-1)$ but also two polynomials $\lambda(x)$ and $\eta(x)$ such that $\lambda\Lambda_r\bar{S} - \eta(x^n-1) = \gcd(\Lambda_r\bar{S}, x^n-1)$. At each intermediate step a new remainder r_i is computed, with decreased degree, together with two intermediate polynomials $\lambda_i(x)$ and $\eta_i(x)$ such that $\lambda_i\Lambda_r\bar{S} - \eta_i(x^n-1) = r_i$. Truncating this algorithm at a proper point we can get a pair of polynomials λ_i and η_i such that $\lambda_i\Lambda_r\bar{S} - \eta_i(x^n-1)$ has degree as small as desired (in particular, smaller than $n-\frac{d-s}{2}$). Algorithm 1 is the truncated Euclidean algorithm. It satisfies that, for all $i \geq 0$, $\deg(r_i) \leq \deg(r_{i-1})$ and $\deg(f_i) \geq \deg(f_{i-1})$.

Algorithm 1

```
Initialize:
    $\begin{pmatrix} r_{-1} & f_{-1} & \varphi_{-1} \\ r_{-2} & f_{-2} & \varphi_{-2} \end{pmatrix} = \begin{pmatrix} -(x^n-1) & 0 & 1 \\ \Lambda_r\bar{S} & 1 & 0 \end{pmatrix}$
while deg$(r_i) \geq n - \frac{d-s}{2}$:
    $q_i =$ Quotient$(r_{i-2}, r_{i-1})$
    $\begin{pmatrix} r_i & f_i & \varphi_i \\ r_{i-1} & f_{i-1} & \varphi_{i-1} \end{pmatrix} = \begin{pmatrix} -q_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{i-1} & f_{i-1} & \varphi_{i-1} \\ r_{i-2} & f_{i-2} & \varphi_{i-2} \end{pmatrix}$
    end while
    Return $f_i/\mathbf{LC}(f_i)$, $\varphi_i/\mathbf{LC}(f_i)$
```

Theorem 2. *If a codeword $c \in C(k)$ is transmitted and s erasures and t errors occur with $2t+s<d$ then the algorithm outputs Λ_e and Ω.*

For all $i \geq -1$ consider the matrices $\begin{pmatrix} \mathring{R}_i & \mathring{F}_i & \mathring{\Phi}_i \\ \mathring{\tilde{R}}_i & \mathring{\tilde{F}}_i & \mathring{\tilde{\Phi}}_i \end{pmatrix} = \begin{pmatrix} 1/\mathrm{LC}(r_i) & 0 \\ 0 & -\mathrm{LC}(r_i) \end{pmatrix} \begin{pmatrix} r_i & f_i & \varphi_i \\ r_{i-1} & f_{i-1} & \varphi_{i-1} \end{pmatrix}$ Notice that $\mathring{R}_i$ is monic. The update step in the algorithm can be replaced by

$$\begin{pmatrix} \mathring{R}_i & \mathring{F}_i & \mathring{\Phi}_i \\ \mathring{\tilde{R}}_i & \mathring{\tilde{F}}_i & \mathring{\tilde{\Phi}}_i \end{pmatrix} = \begin{pmatrix} \frac{1}{\mathrm{LC}(\mathring{\tilde{R}}_{i-1} - Q_i \mathring{R}_{i-1})} & 0 \\ 0 & -\mathrm{LC}(\mathring{\tilde{R}}_{i-1} - Q_i \mathring{R}_{i-1}) \end{pmatrix} \begin{pmatrix} -Q_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mathring{R}_{i-1} & \mathring{F}_{i-1} & \mathring{\Phi}_{i-1} \\ \mathring{\tilde{R}}_{i-1} & \mathring{\tilde{F}}_{i-1} & \mathring{\tilde{\Phi}}_{i-1} \end{pmatrix},$$

where Q_i is the quotient of $\mathring{\tilde{R}}_{i-1}$ by $\mathring{R}_{i-1}$. Moreover, if $Q_i = Q_i^{(0)} + Q_i^{(1)}x + \cdots + Q_i^{(l_i)}x^{l_i}$, then $\begin{pmatrix} -Q_i & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -Q_i^{(0)} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -Q_i^{(1)}x \\ 0 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & -Q_i^{(l)}x^l \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and the update step becomes

$$\begin{pmatrix} \mathring{R}_i & \mathring{F}_i & \mathring{\Phi}_i \\ \mathring{\tilde{R}}_i & \mathring{\tilde{F}}_i & \mathring{\tilde{\Phi}}_i \end{pmatrix} = \begin{pmatrix} \frac{1}{\mathrm{LC}(\mathring{\tilde{R}}_{i-1} - Q_i \mathring{R}_{i-1})} & 0 \\ 0 & -\mathrm{LC}(\mathring{\tilde{R}}_{i-1} - Q_i \mathring{R}_{i-1}) \end{pmatrix} \begin{pmatrix} 1 & -Q_i^{(0)} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -Q_i^{(1)}x \\ 0 & 1 \end{pmatrix} \cdots$$

$$\cdots \begin{pmatrix} 1 & -Q_i^{(l)}x^l \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mathring{R}_{i-1} & \mathring{F}_{i-1} & \mathring{\Phi}_{i-1} \\ \mathring{\tilde{R}}_{i-1} & \mathring{\tilde{F}}_{i-1} & \mathring{\tilde{\Phi}}_{i-1} \end{pmatrix},$$

It can be easily shown that $\mathrm{LC}(\mathring{\tilde{R}}_{i-1} - Q_i \mathring{R}_{i-1})$ as well as all the $Q_i^{(j)}$'s, are the LC of the left-most, top-most element in the previous product of all the previous matrices. This is because $\mathring{R}_i$ is monic. If we define μ to be the (changing) LC of the left-most, top-most element in the product of all the previous matrices, then $\begin{pmatrix} \mathring{R}_i & \mathring{F}_i & \mathring{\Phi}_i \\ \mathring{\tilde{R}}_i & \mathring{\tilde{F}}_i & \mathring{\tilde{\Phi}}_i \end{pmatrix}$ equals

$$\begin{pmatrix} \frac{1}{\mu} & 0 \\ 0 & -\mu \end{pmatrix} \begin{pmatrix} 1 & -\mu \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -\mu x \\ 0 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & -\mu x^{l_i} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mathring{R}_{i-1} & \mathring{F}_{i-1} & \mathring{\Phi}_{i-1} \\ \mathring{\tilde{R}}_{i-1} & \mathring{\tilde{F}}_{i-1} & \mathring{\tilde{\Phi}}_{i-1} \end{pmatrix} =$$

$$\begin{pmatrix} \frac{1}{\mu} & 0 \\ 0 & -\mu \end{pmatrix} \overbrace{\begin{pmatrix} 1 & -\mu \\ 0 & 1 \end{pmatrix}}^{M_m} \overbrace{\begin{pmatrix} 1 & -\mu x \\ 0 & 1 \end{pmatrix}}^{M_{m-1}} \cdots \begin{pmatrix} 1 & -\mu x^{l_i-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -\mu x^{l_i} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -\mu \\ 1/\mu & 0 \end{pmatrix}$$

$$\vdots$$

$$\overbrace{\begin{pmatrix} 1 & -\mu \\ 0 & 1 \end{pmatrix}}^{M_{l_0}} \overbrace{\begin{pmatrix} 1 & -\mu x \\ 0 & 1 \end{pmatrix}}^{M_{l_0-1}} \cdots \overbrace{\begin{pmatrix} 1 & -\mu x^{l_0-1} \\ 0 & 1 \end{pmatrix}}^{M_1} \overbrace{\begin{pmatrix} 1 & -\mu x^{l_0} \\ 0 & 1 \end{pmatrix}}^{M_0} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \mathring{R}_{-1} & \mathring{F}_{-1} & \mathring{\Phi}_{-1} \\ \mathring{\tilde{R}}_{-1} & \mathring{\tilde{F}}_{-1} & \mathring{\tilde{\Phi}}_{-1} \end{pmatrix}$$

Let us define now,

$$\begin{pmatrix} R_{-1} & F_{-1} & \Phi_{-1} \\ \tilde{R}_{-1} & \tilde{F}_{-1} & \tilde{\Phi}_{-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mathring{R}_{-1} & \mathring{F}_{-1} & \mathring{\Phi}_{-1} \\ \mathring{\tilde{R}}_{-1} & \mathring{\tilde{F}}_{-1} & \mathring{\tilde{\Phi}}_{-1} \end{pmatrix} = \begin{pmatrix} \Lambda_r\bar{S} & 1 & 0 \\ x^n - 1 & 0 & -1 \end{pmatrix}$$

$$\begin{pmatrix} R_i & F_i & \Phi_i \\ \tilde{R}_i & \tilde{F}_i & \tilde{\Phi}_i \end{pmatrix} = M_i \cdot M_{i-1} \cdot \cdots \cdot M_0 \cdot \begin{pmatrix} R_{-1} & F_{-1} & \Phi_{-1} \\ \tilde{R}_{-1} & \tilde{F}_{-1} & \tilde{\Phi}_{-1} \end{pmatrix}$$

One can prove that now $\tilde{R}_i$ and F_i are monic for all $i \leq m$. Algorithm 2 computes the matrices $\begin{pmatrix} R_i & F_i & \Phi_i \\ \tilde{R}_i & \tilde{F}_i & \tilde{\Phi}_i \end{pmatrix}$ until $\deg(R_i) < n - \frac{d-s}{2}$.

Algorithm 2

```
Initialize:
    $\begin{pmatrix} R_{-1} & F_{-1} & \Phi_{-1} \\ \tilde{R}_{-1} & \tilde{F}_{-1} & \tilde{\Phi}_{-1} \end{pmatrix} = \begin{pmatrix} \Lambda_r\bar{S} & 1 & 0 \\ x^n - 1 & 0 & -1 \end{pmatrix}$
while $\mathbf{deg}(R_i) \geq n - \frac{d-s}{2}$:
    $\mu = \mathbf{LC}(R_i)$
    $p = \mathbf{deg}(R_i) - \mathbf{deg}(\tilde{R}_i)$
    if $p \geq 0$ then
        $\begin{pmatrix} R_{i+1} & F_{i+1} & \Phi_{i+1} \\ \tilde{R}_{i+1} & \tilde{F}_{i+1} & \tilde{\Phi}_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & -\mu x^p \\ 0 & 1 \end{pmatrix} \begin{pmatrix} R_i & F_i & \Phi_i \\ \tilde{R}_i & \tilde{F}_i & \tilde{\Phi}_i \end{pmatrix}$
    else
        $\begin{pmatrix} R_{i+1} & F_{i+1} & \Phi_{i+1} \\ \tilde{R}_{i+1} & \tilde{F}_{i+1} & \tilde{\Phi}_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & -\mu \\ 1/\mu & 0 \end{pmatrix} \begin{pmatrix} R_i & F_i & \Phi_i \\ \tilde{R}_i & \tilde{F}_i & \tilde{\Phi}_i \end{pmatrix}$
    end if
end while
Return $F_i$, $\Phi_i$
```

After each step corresponding to $p < 0$ the new p is exactly the previous one with opposite sign and so is μ. This is because the polynomials $\tilde{R}_i$ are monic. So, we can join each step corresponding to $p < 0$ with the next one and get that, in this case, $\begin{pmatrix} R_{i+1} & F_{i+1} & \Phi_{i+1} \\ \tilde{R}_{i+1} & \tilde{F}_{i+1} & \tilde{\Phi}_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & \mu x^{-p} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -\mu \\ 1/\mu & 0 \end{pmatrix} \begin{pmatrix} R_i & F_i & \Phi_i \\ \tilde{R}_i & \tilde{F}_i & \tilde{\Phi}_i \end{pmatrix}$

This modification does not alter the output F_i, Φ_i. Furthermore, the only reason to keep the polynomials R_i (and $\tilde{R}_i$) is that we need to compute their leading coefficients (the μ_i's). One can show that $\mathrm{LC}(R_i) = \mathrm{LC}(F_i\Lambda_r\bar{S})$, and so these leading coefficients may be obtained without reference to the polynomials R_i. This allows us to compute the F_i, Φ_i iteratively and dispense with the polynomials R_i.

Algorithm 2 can be transformed in a way such that the remainders are not kept but their degrees. We use $d_i, \tilde{d_i}$ which satisfy at each step $d_i \geq \deg(R_i)$, $\tilde{d_i} = \deg(\tilde{R}_i)$.

Algorithm 3

```
Initialize:
    $d_{-1} = s + \mathbf{deg}(\bar{S})$
    $\tilde{d}_{-1} = n$
    $\begin{pmatrix} F_{-1} & \Phi_{-1} \\ \tilde{F}_{-1} & \tilde{\Phi}_{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
while $d_i \geq n - \frac{d-s}{2}$:
    $\mu = \mathbf{Coefficient}(F_i \Lambda_r \bar{S}, d_i)$
    $p = d_i - \tilde{d}_i$
    if $p \geq 0$ or $\mu = 0$ then
        $\begin{pmatrix} F_{i+1} & \Phi_{i+1} \\ \tilde{F}_{i+1} & \tilde{\Phi}_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & -\mu x^p \\ 0 & 1 \end{pmatrix} \begin{pmatrix} F_i & \Phi_i \\ \tilde{F}_i & \tilde{\Phi}_i \end{pmatrix}$
        $d_{i+1} = d_i - 1$
        $\tilde{d}_{i+1} = \tilde{d}_i$
    else
        $\begin{pmatrix} F_{i+1} & \Phi_{i+1} \\ \tilde{F}_{i+1} & \tilde{\Phi}_{i+1} \end{pmatrix} = \begin{pmatrix} x^{-p} & -\mu \\ 1/\mu & 0 \end{pmatrix} \begin{pmatrix} F_i & \Phi_i \\ \tilde{F}_i & \tilde{\Phi}_i \end{pmatrix}$
        $d_{i+1} = \tilde{d}_i - 1$
        $\tilde{d}_{i+1} = d_i$
    end if
end while
Return $F_i, \Phi_i$
```

Algorithm 3 is exactly the Berlekamp-Massey algorithm that solves the linear recurrence $\sum_{j=0}^{t} \Lambda_j e(\alpha^{i+j-1}) = 0$ for all $i > 0$. This recurrence is derived from $\Lambda \frac{S}{x^n - 1}$ being a polynomial and thus having no terms of negative order in its expression as a Laurent series in $1/x$, and from the equality $\frac{S}{x^n-1} = \frac{1}{x}\left(e(1) + \frac{e(\alpha)}{x} + \frac{e(\alpha^2)}{x^2} + \cdots\right)$.

References

[1] Elwyn R. Berlekamp. *Algebraic coding theory*. McGraw-Hill Book Co., New York, 1968.

[2] Jean-Louis Dornstetter. On the equivalence between Berlekamp's and Euclid's algorithms. *IEEE Trans. Inform. Theory*, 33(3):428–431, 1987.

[3] G. D. Forney, Jr. On decoding BCH codes. *IEEE Trans. Inform. Theory*, IT-11:549–557, 1965.

[4] Agnes E. Heydtmann and Jørn M. Jensen. On the equivalence of the Berlekamp-Massey and the Euclidean algorithms for decoding. *IEEE Trans. Inform. Theory*, 46(7):2614–2624, 2000.

[5] James L. Massey. Shift-register synthesis and BCH decoding. *IEEE Trans. Information Theory*, IT-15:122–127, 1969.

[6] T. D. Mateer. On the equivalence of the Berlekamp-Massey and the Euclidean algorithms for algebraic decoding. In *12th Canadian Workshop on Inf. Theory (CWIT)* pp. 139–142, 2011.

[7] Yasuo Sugiyama, Masao Kasahara, Shigeichi Hirasawa, and Toshihiko Namekawa. A method for solving key equation for decoding Goppa codes. *Information and Control*, 27:87–99, 1975.

On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes

J. Borges[1], C. Fernández-Córdoba[1], R. Ten-Valls[1]

[1] *Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, Spain, {joaquim.borges, cristina.fernandez, roger.ten}@uab.cat*

This work has been partially supported by the Spanish MEC grant TIN2013-40524-P and by the Catalan AGAUR grant 2014SGR-691.

The $\mathbb{Z}_2\mathbb{Z}_4$-additive codes has been introduced in [3] and intensively studied during last years. Recently, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes has been defined in [1] and identified as $\mathbb{Z}_4[x]$-modules of a certain ring. The duality of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes has been studied in [5].

In recent times, $\mathbb{Z}_2\mathbb{Z}_4$-additive codes were generalized to $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additives codes in [2]. They determine, in particular, the standard forms of generator and parity-check matrices and present some bounds on the minimum distance.

Let $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$ be the rings of integers modulo p^r and p^s, respectively, with p prime and $r \leq s$. Since the residue field of $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$ is $\mathbb{Z}_p$, then an element b of $\mathbb{Z}_{p^r}$ could be written uniquely as $b = b_0 + pb_1 + p^2b_2 + \cdots + p^{r-1}b_{r-1}$, and any element $a \in \mathbb{Z}_{p^s}$ as $a = a_0 + pa_1 + p^2a_2 + \cdots + p^{s-1}a_{s-1}$, where $b_i, a_j \in \mathbb{Z}_p$.

Then we can consider the surjective ring homomorphism $\pi : \mathbb{Z}_{p^s} \twoheadrightarrow \mathbb{Z}_{p^r}$, where $\pi(a) = a \mod p^r$.

Note that $\pi(p^i) = 0$ if $i \geq r$. Let $a \in \mathbb{Z}_{p^s}$ and $b \in \mathbb{Z}_{p^r}$. We define a multiplication $*$ as follows: $a * b = \pi(a)b$. Then, $\mathbb{Z}_{p^r}$ is a $\mathbb{Z}_{p^s}$-module with external multiplication given by π. Since $\mathbb{Z}_{p^r}$ is commutative, then $*$ has the commutative property. Then, we can generalize this multiplication over the ring $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ as follows. Let a be an element of $\mathbb{Z}_{p^s}$ and $\mathbf{u} = (u \mid u') = (u_0, u_1, \ldots, u_{\alpha-1} \mid u'_0, u'_1, \ldots, u'_{\beta-1}) \in \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$. Then, $a * \mathbf{u} = (\pi(a)u_0, \pi(a)u_1, \ldots, \pi(a)u_{\alpha-1} \mid au'_0, au'_1, \ldots, au'_{\beta-1})$. With this external operation the ring $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ is also a $\mathbb{Z}_{p^s}$-module.

Definition 1. *A $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive code $\mathscr{C}$ is a $\mathbb{Z}_{p^s}$-submodule of $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$.*

The structure of the generator matrices in standard form and the type of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additives codes are defined and determinated in [2].

Let $\mathscr{C}_\alpha$ be the canonical projection of $\mathscr{C}$ on the first α coordinates and $\mathscr{C}_\beta$ on the last β coordinates. The canonical projection is a linear map. Then, $\mathscr{C}_\alpha$ and $\mathscr{C}_\beta$ are $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$ linear codes of length α and β, respectively. A code $\mathscr{C}$ is called *separable* if $\mathscr{C}$ is the direct product of $\mathscr{C}_\alpha$ and $\mathscr{C}_\beta$, i.e., $\mathscr{C} = \mathscr{C}_\alpha \times \mathscr{C}_\beta$.

Since $r \leq s$, we consider the inclusion map

$$\begin{array}{cccc} \iota: & \mathbb{Z}_{p^r} & \hookrightarrow & \mathbb{Z}_{p^s} \\ & b & \mapsto & b \end{array}.$$

Let $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$, then the inner product is defined [2] as

$$\mathbf{u} \cdot \mathbf{v} = p^{s-r} \sum_{i=0}^{\alpha-1} \iota(u_i v_i) + \sum_{j=0}^{\beta-1} u'_j v'_j \in \mathbb{Z}_{p^s},$$

and the dual code of a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive code $\mathscr{C}$ in $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ is defined in a natural way as

$$\mathscr{C}^{\perp} = \{\mathbf{v} \in \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta} | \mathbf{u} \cdot \mathbf{v} = 0, \forall \mathbf{u} \in \mathscr{C}\}.$$

Let $\mathscr{C}$ be a separable code, then $\mathscr{C}^{\perp}$ is also separable and $\mathscr{C}^{\perp} = \mathscr{C}_{\alpha}^{\perp} \times \mathscr{C}_{\beta}^{\perp}$.

$\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes

Definition 2. *Let $\mathscr{C} \subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive code. The code $\mathscr{C}$ is called* cyclic *if*

$$(u_0, u_1, \ldots, u_{\alpha-2}, u_{\alpha-1} \mid u'_0, u'_1, \ldots, u'_{\beta-2}, u'_{\beta-1}) \in \mathscr{C}$$

implies

$$(u_{\alpha-1}, u_0, u_1, \ldots, u_{\alpha-2} \mid u'_{\beta-1}, u'_0, u'_1, \ldots, u'_{\beta-2}) \in \mathscr{C}.$$

Let $\mathbf{u} = (u_0, u_1, \ldots, u_{\alpha-1} \mid u'_0, \ldots, u'_{\beta-1})$ be a codeword in $\mathscr{C}$ and let i be an integer. Then we denote by $\mathbf{u}^{(i)} = (u_{0-i}, u_{1-i}, \ldots, u_{\alpha-1-i} \mid u'_{0-i}, \ldots, u'_{\beta-1-i})$ the ith shift of $\mathbf{u}$, where the subscripts are read modulo α and β, respectively.

Note that $\mathscr{C}_{\alpha}$ and $\mathscr{C}_{\beta}$ are $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$ cyclic codes of length α and β.

In the particular case that $r = s$, the simultaneous shift of two sets of coordinates that leave invariant the code $\mathscr{C} \subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^r}^{\beta}$ is known in the literature as *double cyclic code* over $\mathbb{Z}_{p^r}$, see [4], [8]. The term *double cyclic* is given in order to distinguish the cyclic code $\mathscr{C} \subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^r}^{\beta}$ to the cyclic code $\mathscr{C}' \subseteq \mathbb{Z}_{p^r}^{\alpha+\beta}$.

Denote by $\mathscr{R}_{r,s}^{\alpha,\beta}$ the ring $\mathbb{Z}_{p^r}[x]/(x^{\alpha}-1) \times \mathbb{Z}_{p^s}[x]/(x^{\beta}-1)$. There is a bijective map between $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ and $\mathscr{R}_{r,s}^{\alpha,\beta}$ given by:

$$(u_0, u_1, \ldots, u_{\alpha-1} \mid u'_0, \ldots, u'_{\beta-1}) \mapsto (u_0 + u_1 x + \cdots + u_{\alpha-1} x^{\alpha-1} \mid u'_0 + \cdots + u'_{\beta-1} x^{\beta-1}).$$

We denote the image of the vector $\mathbf{u}$ by $\mathbf{u}(x)$. Note that we can extend the maps ι and π to the polynomial rings $\mathbb{Z}_{p^r}[x]$ and $\mathbb{Z}_{p^s}[x]$ applying this map to each of the coefficients of a given polynomial.

Definition 3. *Define the operation* $* : \mathbb{Z}_{p^s}[x] \times \mathscr{R}_{r,s}^{\alpha,\beta} \to \mathscr{R}_{r,s}^{\alpha,\beta}$ *as*

$$\lambda(x) * (u(x) \mid u'(x)) = (\pi(\lambda(x))u(x) \mid \lambda(x)u'(x)),$$

where $\lambda(x) \in \mathbb{Z}_{p^s}[x]$ *and* $(u(x) \mid u'(x)) \in \mathscr{R}_{r,s}^{\alpha,\beta}$.

The ring $\mathscr{R}_{r,s}^{\alpha,\beta}$ with the external operation $*$ is a $\mathbb{Z}_{p^s}[x]$-module. Let $\mathbf{u}(x) = (u(x) \mid u'(x))$ be an element of $\mathscr{R}_{r,s}^{\alpha,\beta}$. Note that if we operate $\mathbf{u}(x)$ by x we get

$$\begin{aligned} x * \mathbf{u}(x) &= x * (u(x) \mid u'(x)) \\ &= (u_0 x + \cdots + u_{\alpha-2}x^{\alpha-1} + u_{\alpha-1}x^{\alpha} \mid u'_0 x + \cdots + u'_{\beta-2}x^{\beta-1} + u'_{\beta-1}x^{\beta}) \\ &= (u_{\alpha-1} + u_0 x + \cdots + u_{\alpha-2}x^{\alpha-1} \mid u'_{\beta-1} + u'_0 x + \cdots + u'_{\beta-2}x^{\beta-1}). \end{aligned}$$

Hence, $x * \mathbf{u}(x)$ is the image of the vector $\mathbf{u}^{(1)}$. Thus, the operation of $\mathbf{u}(x)$ by x in $\mathscr{R}_{r,s}^{\alpha,\beta}$ corresponds to a shift of $\mathbf{u}$. In general, $x^i * \mathbf{u}(x) = \mathbf{u}^{(i)}(x)$ for all i.

Now, we study submodules of $\mathscr{R}_{r,s}^{\alpha,\beta}$. We describe the generators of such submodules and state some properties. From now on, $\langle S \rangle$ will denote the $\mathbb{Z}_{p^s}[x]$-submodule generated by a subset S of $\mathscr{R}_{r,s}^{\alpha,\beta}$.

For the rest of the discussion we will consider that α and β are coprime integers with p. From this assumption we know that $\mathbb{Z}_{p^r}[x]/(x^\alpha - 1)$ and $\mathbb{Z}_{p^s}[x]/(x^\beta - 1)$ are principal ideal rings, see [6],[7].

Theorem 4. *The* $\mathbb{Z}_{p^s}[x]$*-module* $\mathscr{R}_{r,s}^{\alpha,\beta}$ *is noetherian, and every submodule* $\mathscr{C}$ *of* $\mathscr{R}_{r,s}^{\alpha,\beta}$ *can be written as*

$$\mathscr{C} = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle,$$

where $b(x), a(x)$ *are generator polynomials in* $\mathbb{Z}_{p^r}[x]/(x^\alpha - 1)$ *and* $\mathbb{Z}_{p^s}[x]/(x^\beta - 1)$ *resp., and* $\ell(x) \in \mathbb{Z}_{p^r}[x]/(x^\alpha - 1)$.

From the previous results, it is clear that we can identify codes in $\mathbb{Z}_{p^r}^\alpha \times \mathbb{Z}_{p^s}^\beta$ that are cyclic as submodules of $\mathscr{R}_{r,s}^{\alpha,\beta}$. So, any submodule of $\mathscr{R}_{r,s}^{\alpha,\beta}$ is a cyclic code. From now on, we will denote by $\mathscr{C}$ indistinctly both the code and the corresponding submodule.

Proposition 5. *Let* $\mathscr{C} \subseteq \mathbb{Z}_{p^r}^\alpha \times \mathbb{Z}_{p^s}^\beta$ *be a* $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$*-additive cyclic code. Then, there exist polynomials* $\ell(x)$ *and* $b_0(x)|b_1(x)|\ldots|b_{r-1}(x)|(x^\alpha - 1)$ *over* $\mathbb{Z}_{p^r}[x]$*, and polynomials* $a_0(x)|a_1(x)|\cdots|a_{s-1}(x)|(x^\beta - 1)$ *over* $\mathbb{Z}_{p^s}[x]$ *such that*

$$\mathscr{C} = \langle (b_0(x) + pb_1(x) + \cdots + p^{r-1}b_{r-1}(x) \mid 0), (\ell(x) \mid a_0(x) + pa_1(x) + \cdots + p^{s-1}a_{s-1}(x)) \rangle.$$

Let $b(x)=b_0(x)+pb_1(x)+\cdots+p^{r-1}b_{r-1}(x)$ and $a(x)=a_0(x)+pa_1(x)+\cdots+p^{s-1}a_{s-1}(x)$, for polynomials $b_i(x)$ and $a_j(x)$ as in Proposition 5. Then, for the rest of the discussion, we assume that a cyclic code $\mathscr{C}$ over $\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}$ is generated by $\langle(b(x)\mid 0),(\ell(x)\mid a(x))\rangle$. Since $b_0(x)$ is a factor of $x^{\alpha}-1$ and for $i=1\dots r-1$ the polynomial $b_i(x)$ is a factor of $b_{i-1}(x)$, we will denote $\hat{b}_0(x)=\frac{x^{\alpha}-1}{b_0(x)}$ and $\hat{b}_i(x)=\frac{b_{i-1}(x)}{b_i(x)}$ for $i=1\dots r-1$. In the same way, we define $\hat{a}_0(x)=\frac{x^{\beta}-1}{a_0(x)}$, $\hat{a}_j(x)=\frac{a_{j-1}(x)}{a_j(x)}$ for $j=1\dots s-1$.

Proposition 6. *Let $\mathscr{C}\subseteq\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Then,*

$$\prod_{t=0}^{s-1}\hat{a}_t(x)*(\ell(x)\mid a(x))\in\langle(b(x)\mid 0)\rangle.$$

Theorem 7. *Let $\mathscr{C}\subseteq\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Define*

$$B_{p^j}=\left[x^i(\prod_{t=0}^{j-1}\hat{b}_t(x))(b(x)\mid 0)\right]_{i=0}^{\deg(\hat{b}_j(x))-1},$$

for $0\leq j\leq r-1$, and

$$A_{p^k}=\left[x^i(\prod_{t=0}^{k-1}\hat{a}_t(x))(\ell(x)\mid a(x))\right]_{i=0}^{\deg(\hat{a}_k(x))-1},$$

for $0\leq k\leq s-1$. Then,

$$S=\bigcup_{j=0}^{r-1}B_{p^j}\bigcup_{t=0}^{s-1}A_{p^t}$$

forms a minimal generating set for $\mathscr{C}$ as a $\mathbb{Z}_{p^s}$-module. Moreover,

$$|\mathscr{C}|=p^{\sum_{i=0}^{r-1}(r-i)\deg(\hat{b}_i(x))+\sum_{j=0}^{s-1}(s-j)\deg\hat{a}_j(x)}.$$

Let $\mathscr{C}$ be a cyclic code and $\mathscr{C}^{\perp}$ the dual code of $\mathscr{C}$. Taking a vector $\mathbf{v}$ of $\mathscr{C}^{\perp}$, $\mathbf{u}\cdot\mathbf{v}=0$ for all $\mathbf{u}$ in $\mathscr{C}$. Since $\mathbf{u}$ belongs to $\mathscr{C}$, we know that $\mathbf{u}^{(-1)}$ is also a codeword. So, $\mathbf{u}^{(-1)}\cdot\mathbf{v}=\mathbf{u}\cdot\mathbf{v}^{(1)}=0$ for all $\mathbf{u}$ from $\mathscr{C}$, therefore $\mathbf{v}^{(1)}$ is in $\mathscr{C}^{\perp}$ and $\mathscr{C}^{\perp}$ is also a cyclic code over $\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}$. Consequently, we obtain the following proposition.

Proposition 8. *Let $\mathscr{C}\subseteq\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Then the dual code of $\mathscr{C}$ is also a cyclic code in $\mathbb{Z}_{p^r}^{\alpha}\times\mathbb{Z}_{p^s}^{\beta}$.*

Proposition 9. *Let $\mathscr{C} \subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Then,*

$$|\mathscr{C}^{\perp}| = p^{\sum_{i=1}^{r} i \deg(\hat{b}_i(x)) + \sum_{j=1}^{s} j \deg(\hat{a}_j(x))}.$$

The *reciprocal polynomial* of a polynomial $p(x)$ is $x^{\deg(p(x))}p(x^{-1})$ and is denoted by $p^*(x)$. We denote the polynomial $\sum_{i=0}^{m-1} x^i$ by $\theta_m(x)$, and the least common multiple of α and β by $\mathfrak{m}$.

Definition 10. *Let $\mathbf{u}(x) = (u(x) \mid u'(x))$ and $\mathbf{v}(x) = (v(x) \mid v'(x))$ be elements in $\mathscr{R}_{r,s}^{\alpha,\beta}$. We define the map $\circ : \mathscr{R}_{r,s}^{\alpha,\beta} \times \mathscr{R}_{r,s}^{\alpha,\beta} \longrightarrow \mathbb{Z}_{p^s}[x]/(x^{\mathfrak{m}} - 1)$, such that*

$$\begin{aligned} \circ(\mathbf{u}(x), \mathbf{v}(x)) =& p^{s-r}\iota(u(x)v^*(x))\theta_{\frac{\mathfrak{m}}{r}}(x^r)x^{\mathfrak{m}-1-\deg(v(x))} + \\ &+ u'(x)v'^*(x)\theta_{\frac{\mathfrak{m}}{s}}(x^s)x^{\mathfrak{m}-1-\deg(v'(x))} \mod (x^{\mathfrak{m}} - 1). \end{aligned}$$

The map $\circ$ is linear in each of its arguments; i.e., if we fix the first entry of the map invariant, while letting the second entry vary, then the result is a linear map. Similarly, when fixing the second entry invariant. Then, the map $\circ$ is a bilinear map between $\mathbb{Z}_{p^s}[x]$-modules.

From now on, we denote $\circ(\mathbf{u}(x), \mathbf{v}(x))$ by $\mathbf{u}(x) \circ \mathbf{v}(x)$. Note that $\mathbf{u}(x) \circ \mathbf{v}(x)$ belongs to $\mathbb{Z}_{p^s}[x]/(x^{\mathfrak{m}} - 1)$.

Theorem 11. *Let $\mathbf{u}$ and $\mathbf{v}$ be vectors in $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ with associated polynomials $\mathbf{u}(x) = (u(x) \mid u'(x))$ and $\mathbf{v}(x) = (v(x) \mid v'(x))$, respectively. Then, $\mathbf{v}$ is orthogonal to $\mathbf{u}$ and all its shifts if and only if*

$$\mathbf{u}(x) \circ \mathbf{v}(x) = 0 \mod (x^{\mathfrak{m}} - 1).$$

References

[1] T. Abualrub, I. Siap, N. Aydin. $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. *IEEE Trans. Info. Theory*, vol. 60, No. 3, pp. 1508-1514, 2014.

[2] I. Aydogdu, I. Siap. On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes. Linear and Multilinear Algebra, DOI: 10.1080/03081087.2014.952728, 2014.

[3] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà and M. Villanueva. $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality. *Designs, Codes and Cryptography*, vol. 54, No. 2, pp. 167-179, 2010.

[4] J. Borges, C. Fernández-Córdoba, R. Ten-Valls. $\mathbb{Z}_2$-double cyclic codes. arXiv:1410.5604, 2014.

[5] J. Borges, C. Fernández-Córdoba, R. Ten-Valls. $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, generator polynomials and dual codes. arXiv:1406.4425, 2014.

[6] A.R. Calderbank, N.J.A. Sloane. Modular and p-adic cyclic codes. *Designs, Codes and Cryptography*, vol. 37, No. 6, pp. 21-35, 1995.

[7] H.Q. Dinh, S.R. López-Permouth Cyclic and negacyclic codes over finite chain rings. *Lecture Notes in Computer Science*, n. 5228, pp. 46-55, 2008.

[8] J. Gao, M. Shi, T. Wu and F. Fu. On double cyclic codes over $\mathbb{Z}_4$. arXiv: 1501.01360, 2015.

PD-sets for (nonlinear) Hadamard Z_4-linear codes

R. D. Barrolleta[1], M. Villanueva[1]

[1] *Universitat Autònoma de Barcelona, Spain, {rolanddavid.barrolleta, merce.villanueva}@uab.cat*

This work was partially supported by the Spanish MEC under Grant TIN2013-40524-P, and by the Catalan AGAUR under Grant 2014SGR-691.

Any nonempty subset C of $\mathbb{Z}_2^n$ is a binary code and a subgroup of $\mathbb{Z}_2^n$ is called a *binary linear code*. Equivalently, any nonempty subset $\mathscr{C}$ of $\mathbb{Z}_4^n$ is a quaternary code and a subgroup of $\mathbb{Z}_4^n$ is called a *quaternary linear code*. Quaternary codes can be seen as binary codes under the usual Gray map $\Phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ defined as $\Phi((y_1,\dots,y_n)) = (\phi(y_1),\dots,\phi(y_n))$, where $\phi(0) = (0,0)$, $\phi(1) = (0,1)$, $\phi(2) = (1,1)$, $\phi(3) = (1,0)$, for all $y = (y_1,\dots,y_n) \in \mathbb{Z}_4^n$. If $\mathscr{C}$ is a quaternary linear code, the binary code $C = \Phi(\mathscr{C})$ is said to be a $\mathbb{Z}_4$-*linear code*.

A $\mathbb{Z}_2\mathbb{Z}_4$-*additive code* $\mathscr{C}$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. We consider the extension of the Gray map $\Phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \to \mathbb{Z}_2^{\alpha+2\beta}$ defined as $\Phi(x,y) = (x,\phi(y_1),\dots,\phi(y_\beta))$, for all $x \in \mathbb{Z}_2^\alpha$ and $y = (y_1,\dots,y_\beta) \in \mathbb{Z}_4^\beta$. This generalization allows us to consider $\mathbb{Z}_2\mathbb{Z}_4$-additive codes also as binary codes. If $\mathscr{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, the binary code $C = \Phi(\mathscr{C})$ is said to be a $\mathbb{Z}_2\mathbb{Z}_4$-*linear code*. Moreover, since the code $\mathscr{C}$ is isomorphic to an abelian group $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$, we say that $\mathscr{C}$ (or equivalently the corresponding $\mathbb{Z}_2\mathbb{Z}_4$-linear code $C = \Phi(\mathscr{C})$) is of type $(\alpha,\beta;\gamma,\delta)$ [3]. Note that $\mathbb{Z}_2\mathbb{Z}_4$-additive codes can be seen as a generalization of binary (when $\beta = 0$) and quaternary (when $\alpha = 0$) linear codes. The *permutation automorphism group* of $\mathscr{C}$ and $C = \Phi(\mathscr{C})$, denoted by PAut($\mathscr{C}$) and PAut(C), respectively, is the group generated by all permutations that let the set of codewords invariant.

A binary Hadamard code of length n has $2n$ codewords and minimum distance $n/2$. The $\mathbb{Z}_2\mathbb{Z}_4$-additive codes such that, under the Gray map, give a binary Hadamard code are called $\mathbb{Z}_2\mathbb{Z}_4$-*additive Hadamard codes* and the corresponding $\mathbb{Z}_2\mathbb{Z}_4$-linear codes are called *Hadamard* $\mathbb{Z}_2\mathbb{Z}_4$-*linear codes*, or just *Hadamard* $\mathbb{Z}_4$-*linear codes* when $\alpha = 0$. The permutation automorphism group of $\mathbb{Z}_2\mathbb{Z}_4$-additive Hadamard codes with $\alpha = 0$ was characterized in [9] and the permutation automorphism group of $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes was studied in [6].

Let C be a binary code of length n. For a vector $v \in \mathbb{Z}_2^n$ and a set $I \subseteq \{1,\dots,n\}$, we denote by v_I the restriction of v to the coordinates in I and by C_I the set $\{v_I : v \in C\}$. Suppose that $|C| = 2^k$. A set $I \subseteq \{1,\dots,n\}$ of k coordinate positions is an *information set* for C if $|C_I| = 2^k$. If such I exists, C is said to be a *systematic code*.

Permutation decoding is a technique, introduced by MacWilliams [8], which involves finding a subset S of the permutation automorphism group PAut(C) of a code C in order to assist in decoding. Let C be a systematic t-error-correcting code with information set I. A subset $S \subseteq \mathrm{PAut}(C)$ is an *s-PD-set* for the code C if every s-set of coordinate positions is moved out of the information set I by at least one element of the set S, where $1 \leq s \leq t$. If $s = t$, S is said to be a *PD-set*.

In [4], it is shown how to find s-PD-sets of size $s+1$ that satisfy the Gordon-Schönheim bound for partial permutation decoding for the binary simplex code S_m of length $2^m - 1$, for all $m \geq 4$ and $1 < s \leq \left\lfloor \frac{2^m-m-1}{m} \right\rfloor$. In [1], similar results are establish for the binary linear Hadamard code H_m (extended code of S_m) of length 2^m , for all $m \geq 4$ and $1 < s \leq \left\lfloor \frac{2^m-m-1}{1+m} \right\rfloor$, following the techniques described in [4].

The paper is organized as follows. In Section 1, we show that the Gordon-Schönheim bound can be adapted to systematic codes, not necessarily linear. Moreover, we apply the bound of the minimum size of s-PD-sets for binary Hadamard codes obtained in [1] to Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, which are systematic [2] but not linear in general. In Section 2, we provide a criterion to obtain s-PD-sets of size $s+1$ for $\mathbb{Z}_4$-linear codes. Finally, in Section 3, we recall a recursive construction to obtain all $\mathbb{Z}_2\mathbb{Z}_4$-additive codes with $\alpha = 0$ [7] and we give a recursive method to obtain s-PD-sets for the corresponding Hadamard $\mathbb{Z}_4$-linear codes.

1 Minimum size of s-PD-sets

There is a well-known bound on the minimum size of PD-sets for linear codes based on the length, dimension and minimum distance of such codes that can be adapted for systematic codes (not necessarily linear) easily:

Proposition 1. *Let C be a systematic t-error correcting code of length n, size $|C| = 2^k$ and minimum distance d. Let $r = n-k$ be the redundancy of C. If S is a PD-set for C, then*

$$|S| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil. \tag{1}$$

The above inequality (1) is often called the *Gordon-Schönheim bound*. This result is quoted and proved for linear codes in [5]. We can follow the same proof since the linearity of the code C is only used to guarantee that C is systematic. In [2], it is shown that $\mathbb{Z}_2\mathbb{Z}_4$-linear codes are systematic. Moreover, a systematic encoding is given for these codes.

The Gordon-Schönheim bound can be adapted to s-PD-sets for all s up to the error correcting capability of the code. Note that the error-correcting capability of any Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-linear code of length $n = 2^m$ is $t_m = \lfloor (d-1)/2 \rfloor = 2^{m-2} - 1$. Therefore, the right side of the bound given by (1), for Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-linear codes of length 2^m and for all $1 \leq s \leq t_m$, becomes

$$g_m(s) = \left\lceil \frac{2^m}{2^m-m-1} \left\lceil \frac{2^m-1}{2^m-m-2} \left\lceil \cdots \left\lceil \frac{2^m-s+1}{2^m-m-s} \right\rceil \right\rceil \cdots \right\rceil \right\rceil. \tag{2}$$

For any $m \geq 4$ and $1 \leq s \leq t_m$, we have that $g_m(s) \geq s+1$. The smaller the size of the PD-set is, the more efficient permutation decoding becomes. Because of this, we will focus on the case when $g_m(s) = s+1$.

2 s-PD-sets of size $s+1$ for $\mathbb{Z}_4$-linear codes

Let $\mathscr{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(0,\beta;\gamma,\delta)$ and let $C = \Phi(\mathscr{C})$ be the corresponding $\mathbb{Z}_4$-linear code. Let $\Phi : \mathrm{PAut}(\mathscr{C}) \to \mathrm{PAut}(C)$ be the map defined as

$$\Phi(\tau)(i) = \begin{cases} 2\tau(i/2), & \text{if } i \text{ is even,} \\ 2\tau(\frac{i+1}{2}) - 1 & \text{if } i \text{ is odd,} \end{cases}$$

for all $\tau \in \mathrm{Sym}(\beta)$ and $i \in \{1,\ldots,2\beta\}$. The map Φ is a group monomorphism. Given a subset $\mathscr{S}$ of $\mathrm{PAut}(\mathscr{C}) \subseteq \mathrm{Sym}(\beta)$, we define the set $S = \Phi(\mathscr{S}) = \{\Phi(\tau) : \tau \in \mathscr{S}\}$, which is a subset of $\mathrm{PAut}(C) \subseteq \mathrm{Sym}(2\beta)$.

A set $\mathscr{I} = \{i_1,\ldots,i_{\gamma+\delta}\} \subseteq \{1,\ldots,\beta\}$ of $\gamma+\delta$ coordinate positions is said to be a *quaternary information set* for the code $\mathscr{C}$ if the set $\Phi(\mathscr{I})$, defined as $\Phi(\mathscr{I}) = \{2i_1-1, 2i_1, \ldots, 2i_\delta - 1, 2i_\delta, 2i_{\delta+1}-1, \ldots, 2i_{\delta+\gamma}-1\}$, is an information set for $C = \Phi(\mathscr{C})$ for some ordering of elements of $\mathscr{I}$.

Let S be an s-PD-set of size $s+1$. The set S is a *nested* s-PD-set if there is an ordering of the elements of S, $S = \{\sigma_1,\ldots,\sigma_{s+1}\}$, such that $S_i = \{\sigma_1,\ldots,\sigma_{i+1}\} \subseteq S$ is an i-PD-set of size $i+1$, for all $i \in \{1,\ldots,s\}$.

Proposition 2. *Let $\mathscr{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(0,\beta;\gamma,\delta)$ with quaternary information set $\mathscr{I}$ and let s be a positive integer. If $\tau \in \mathrm{PAut}(\mathscr{C})$ has at least $\gamma+\delta$ disjoint cycles of length $s+1$ such that there is exactly one quaternary information position per cycle of length $s+1$, then $S = \{\Phi(\tau^i)\}_{i=1}^{s+1}$ is an s-PD-set of size $s+1$ for the $\mathbb{Z}_4$-linear code $C = \Phi(\mathscr{C})$ with information set $\Phi(\mathscr{I})$. Moreover, any ordering of the elements of S gives a nested r-PD-set for any $r \in \{1,\ldots,s\}$.*

Example 3. *Let $\mathscr{C}_{0,3}$ be the $\mathbb{Z}_2\mathbb{Z}_4$-additive Hadamard code of type $(0,16;0,3)$ with generator matrix*

$$\mathscr{G}_{0,3} = \begin{pmatrix} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3 \\ 0&0&0&0&1&1&1&1&2&2&2&2&3&3&3&3 \end{pmatrix}.$$

Let $\tau = (1,16,11,6)(2,7,12,13)(3,14,9,8)(4,5,10,15) \in \mathrm{PAut}(\mathscr{C}_{0,3}) \subseteq \mathrm{Sym}(16)$ [9]. It is straightforward to check that $\mathscr{I} = \{1,2,5\}$ is a quaternary information set for $\mathscr{C}_{0,3}$. Note that each information position in $\mathscr{I}$ is in a different cycle of τ. Let $\sigma = \Phi(\tau) \in \mathrm{PAut}(C_{0,3}) \subseteq \mathrm{Sym}(32)$, where $C_{0,3} = \Phi(\mathscr{C}_{0,3})$. Thus, by Proposition

2, $S=\{\sigma,\sigma^2,\sigma^3,\sigma^4\}$ *is a 3-PD-set of size 4 for* $C_{0,3}$ *with information set* $I=\{1,2,3,4,9,10\}$. *Note that* $C_{0,3}$ *is the smallest Hadamard* $\mathbb{Z}_4$*-linear code that is a binary nonlinear code.*

3 *s*-PD-sets for Hadamard $\mathbb{Z}_4$-linear codes

Let $\mathbf{0},\mathbf{1},\mathbf{2}$ and $\mathbf{3}$ be the repetition of symbol 0, 1, 2 and 3, respectively. Let $\mathscr{G}_{\gamma,\delta}$ be a generator matrix of the $\mathbb{Z}_2\mathbb{Z}_4$-additive Hadamard code $\mathscr{C}_{\gamma,\delta}$ of length $\beta=2^{m-1}$ and type $(0,\beta;\gamma,\delta)$, where $m=\gamma+2\delta-1$. A generator matrix for the $\mathbb{Z}_2\mathbb{Z}_4$-additive Hadamard code $\mathscr{C}_{\gamma+1,\delta}$ of length $\beta'=2\beta=2^m$ and type $(0,\beta';\gamma+1,\delta)$ can be constructed as follows [7]:

$$\mathscr{G}_{\gamma+1,\delta}=\begin{pmatrix} \mathbf{0} & \mathbf{2} \\ \mathscr{G}_{\gamma,\delta} & \mathscr{G}_{\gamma,\delta} \end{pmatrix}. \tag{3}$$

Equivalently, a generator matrix for the $\mathbb{Z}_2\mathbb{Z}_4$-additive Hadamard code $\mathscr{C}_{\gamma,\delta+1}$ of length $\beta''=4\beta=2^{m+1}$ and type $(0,\beta'';\gamma,\delta+1)$ can be constructed as [7]:

$$\mathscr{G}_{\gamma,\delta+1}=\begin{pmatrix} \mathscr{G}_{\gamma,\delta} & \mathscr{G}_{\gamma,\delta} & \mathscr{G}_{\gamma,\delta} & \mathscr{G}_{\gamma,\delta} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \end{pmatrix}. \tag{4}$$

Note that a generator matrix for every code $\mathscr{C}_{\gamma,\delta}$ can be obtained by applying (3) and (4) recursively over the generator matrix $\mathscr{G}_{0,1}=(1)$ of the code $\mathscr{C}_{0,1}$. From now on, we assume that $\mathscr{C}_{\gamma,\delta}$ is obtained by using these constructions.

Proposition 4. *Let* $\mathscr{C}_{\gamma,\delta}$ *be a* $\mathbb{Z}_2\mathbb{Z}_4$*-additive Hadamard code of type* $(0,\beta;\gamma,\delta)$ *with quaternary information set* $\mathscr{I}$. *The set* $\mathscr{I}\cup\{\beta+1\}$ *is a suitable quaternary information set for both codes* $\mathscr{C}_{\gamma+1,\delta}$ *and* $\mathscr{C}_{\gamma,\delta+1}$ *obtained from* $\mathscr{C}_{\gamma,\delta}$ *by applying constructions (3) and (4), respectively.*

Despite the fact that the quaternary information set is the same for $\mathscr{C}_{\gamma+1,\delta}$ and $\mathscr{C}_{\gamma,\delta+1}$, the information set for the corresponding binary codes $C_{\gamma+1,\delta}$ and $C_{\gamma,\delta+1}$ are $I'=\Phi(\mathscr{I})\cup\{2\beta+1\}$ and $I''=\Phi(\mathscr{I})\cup\{2\beta+1,2\beta+2\}$, respectively.

Given two permutations $\sigma_1\in\mathrm{Sym}(n_1)$ and $\sigma_2\in\mathrm{Sym}(n_2)$, we define the permutation $(\sigma_1|\sigma_2)\in\mathrm{Sym}(n_1+n_2)$, where σ_1 acts on the coordinates $\{1,\ldots,n_1\}$ and σ_2 acts on the coordinates $\{n_1+1,\ldots,n_1+n_2\}$. Given $\sigma_i\in\mathrm{Sym}(n_i)$, $i\in\{1,\ldots,4\}$, we define the permutation $(\sigma_1|\sigma_2|\sigma_3|\sigma_4)$ in the same way.

Proposition 5. *Let S be an s-PD-set of size l for the Hadamard* $\mathbb{Z}_4$*-linear code* $C_{\gamma,\delta}$ *of binary length* $n=2\beta$ *and type* $(0,\beta;\gamma,\delta)$ *with respect to an information set I. Then the set* $(S|S)=\{(\sigma|\sigma):\sigma\in S\}$ *is an s-PD-set of size l with respect to the information set* $I'=I\cup\{n+1\}$ *for the Hadamard* $\mathbb{Z}_4$*-linear code* $C_{\gamma+1,\delta}$ *of binary length* $2n$ *and type* $(0,2\beta;\gamma+1,\delta)$ *constructed from (3) and the Gray map.*

Example 6. *Let S be the 3-PD-set of size 4 for $C_{0,3}$ of binary length 32 with respect to the information set $I = \{1,2,3,4,9,10\}$, given in Example* 3. *By Propositions* 4 *and* 5*, the set $(S|S)$ is a 3-PD-set of size 4 for the Hadamard $\mathbb{Z}_4$-linear code $C_{1,3}$ of binary length 64 with respect to the information set $I' = \{1,2,3,4,9,10,33\}$.*

Proposition 5 can not be generalized directly for Hadamard $\mathbb{Z}_4$-linear codes $C_{\gamma,\delta+1}$ constructed from (4). Note that if S is an s-PD-set for the Hadamard $\mathbb{Z}_4$-linear code $C_{\gamma,\delta}$, then the set $(S|S|S|S) = \{(\sigma|\sigma|\sigma|\sigma) : \sigma \in S\}$ is not in general an s-PD-set for the Hadamard $\mathbb{Z}_4$-linear code $C_{\gamma,\delta+1}$.

Proposition 7. *Let $\mathscr{S} \subseteq \mathrm{PAut}(\mathscr{C}_{\gamma,\delta})$ such that $\Phi(\mathscr{S})$ is an s-PD-set of size l for the Hadamard $\mathbb{Z}_4$-linear code $C_{\gamma,\delta}$ of binary length $n = 2\beta$ and type $(0,\beta;\gamma,\delta)$ with respect to an information set I. Then the set $\Phi((\mathscr{S}|\mathscr{S}|\mathscr{S}|\mathscr{S})) = \{\Phi((\tau|\tau|\tau|\tau)) : \tau \in \mathscr{S}\}$ is an s-PD-set of size l with respect to the information set $I'' = I \cup \{n+1, n+2\}$ for the Hadamard $\mathbb{Z}_4$-linear code $C_{\gamma,\delta+1}$ of binary length* $4n$ *and type $(0,4\beta;\gamma,\delta+1)$ constructed from (4) and the Gray map.*

Example 8. *Let $\mathscr{S} = \{\tau,\tau^2,\tau^3,\tau^4\}$, where τ is defined as in Example 3. By Proposition 7, the set $\Phi((\mathscr{S}|\mathscr{S}|\mathscr{S}|\mathscr{S}))$ is a 3-PD-set of size 4 for the Hadamard $\mathbb{Z}_4$-linear code $C_{0,4}$ of binary length 128 with respect to the information set $I' = \{1,2,3,4,9,10,33,34\}$.*

Propositions 5 and 7 can be applied recursively to acquire s-PD-sets for the infinite family of Hadamard $\mathbb{Z}_4$-linear codes obtained (by using constructions (3) and (4)) from a given Hadamard $\mathbb{Z}_4$-linear code where we already have such set.

References

[1] R. Barrolleta and M. Villanueva, “Partial permutation decoding for binary linear Hadamard codes," *Electronic Notes in Discrete Mathematics*, 46 (2014) 35-42.

[2] J. J. Bernal, J. Borges, C. Fernández-Córboda, and M. Villanueva, “Permutation decoding of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes," *Des. Codes and Cryptogr.*, DOI 10.1007/s10623-014-9946-4, 2014.

[3] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, and M. Villanueva, “$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality," *Des. Codes and Cryptogr.*, vol. 54: 167–179, 2010.

[4] W. Fish, J. D. Key, and E. Mwambene, “Partial permutation decoding for simplex codes," *Advances in Mathematics of Comunications*, vol. 6(4): 505–516, 2012.

[5] W. C. Huffman, *Codes and groups, Handbook of coding theory*, 1998.

[6] D. S. Krotov and M. Villanueva “Classification of the $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes and their automorphism groups," *IEEE Trans. Inf. Theory*, vol. 61(2): 887–894, 2015.

[7] D. S. Krotov, “$\mathbb{Z}_4$-linear Hadamard and extended perfect codes," *Electronic Notes in Discrete Mathematics*, vol. 6 (2001), 107-112.

[8] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 1977.

[9] J. Pernas, J. Pujol and M. Villanueva. “Characterization of the automorphism group of quaternary linear Hadamard Codes," *Des. Codes Cryptogr.*, 70(1-2), 105–115, 2014.

Kronecker sums to construct Hadamard full propelinear codes of type C_nQ_8

J. Rifà[1], E. Suárez Canedo[1]

[1] *Universitat Autònoma de Barcelona, Catalunya, Spain, {josep.rifa,emilio.suarez}@uab.cat*

Hadamard matrices with a subjacent algebraic structure have been deeply studied as well as the links with other topics in algebraic combinatorics [1]. An important and pioneering paper about this subject is [5], where it is introduced the concept of Hadamard group. In addition, we find beautiful equivalences between Hadamard groups, 2-cocyclic matrices and relative difference sets [4], [7]. From the side of coding theory, it is desirable that the algebraic structures we are dealing with preserves the Hamming distance. This is the case of the propelinear codes and specially those which are translation invariant which has been characterized as the image, by a suitable Gray map, of a subgroup of a direct product of $\mathbb{Z}_2$, $\mathbb{Z}_4$ and Q_8 (see [8] and references there).

As for the 2-cocyclic matrices and relative difference sets it was shown in [10] that the concept of Hadamard group is equivalent to Hadamard full propelinear codes (HFP for short). This new equivalence provides a good place to study the rank and the dimension of the kernel of the Hadamard codes we construct. These are important steps trying to solve several conjectures involving Hadamard matrices. In [6] it was introduced a special Hadamard group, called type Q and it was conjectured that Hadamard matrices of this type exists for all possible lengths.

In this paper we are studying Hadamard codes of type C_nQ_8, which are full propelinear and the subjacent group structure is isomorphic to a direct sum of the cyclic group C_n and the quaternion group Q_8. The main results we present are about the links with the Hadamard codes of type Q and the construction of Kronecker sums allowing to duplicate or quadruplicate the length of the code. With the current results we conjecture that it is not possible to go deeper with the Kronecker construction than duplicate or quadruplicate the initial HFP-code, otherwise we contradicts the Ryse conjecture [11] about circulant Hadamard matrices.

1 Introduction

We denote by $\mathbb{Z}_q$, the ring of integers modulo q and by $\mathbb{F}_q$ a finite field with q elements. The Hamming distance between two vectors $x, y \in \mathbb{F}_2$, denoted by $d_H(x,y)$, is the number of coordinates in which they differ, and $wt_H(x)$ is the Hamming weight. We write d for the minimum distance of a code which is equal to its minimum weight when C is linear. A $[n,k,d]$-code C over $\mathbb{F}_q$ is a k-dimensional vector subspace of $\mathbb{F}_q^n$ with minimum distance d. Any subset C of $\mathbb{F}_2^n$ is called a binary code. If the code is not linear we say that a (n,M,d)-code has length n, cardinal M and minimum Hamming distance d. For a vector v in $\mathbb{F}_q^n$, the support of v, denoted by $\mathrm{Supp}\,(v)$, is defined as the set of its nonzero positions. The *rank* of a binary code C is the dimension of the linear span of C. The *kernel* of a binary code is the set of words which keeps the code invariant by translation, $K(C) : \{z \in \mathbb{Z}_2^n : z+C = C\}$. Assuming that the zero vector is in C, the kernel is a linear subspace and we denote by k its dimension.

An Hadamard matrix of order $4n$ is a matrix of size $4n \times 4n$ with entries ± 1, such that $HH^T = 4nI$. Any two rows (columns) of an Hadamard matrix agree in precisely $2n$ components. Two Hadamard matrices are equivalent if one can be obtained from the other by permuting rows and/or columns and multiplying rows and/or columns by -1. With the last operations we can change the first row and column of H into $+1$'s and we obtain an equivalent Hadamard matrix which is called normalized. If $+1$'s are replaced by 0's and -1's by 1's, the initial Hadamard matrix is changed into an (binary) Hadamard matrix and, from now on, we will refer to it when we deal with Hadamard matrices. The binary code consisting of the rows of an (binary) Hadamard matrix and their complements is called an (binary) Hadamard code C_H, which is of length $4n$, with $8n$ codewords, and minimum distance $2n$.

In Section 1 we introduce some basics about the subject. In Section 2, we define the concept of Hadamard full propelinear code and we describe the motivation to work using $C_n \times Q_8$ group structures. In Section 3, we focus our attention to the case of n odd, we compute the rank and the dimension of the kernel and we provide an example of this kind of codes. In Section 4, we use the Kronecker sum construction to duplicate and quadruplicate the length of the initial HFP-code of type C_nQ_8, with n odd, obtaining new HFP-codes of type $C_{2n}Q_8$ and $C_{4n}Q_8$.

2 Hadamard full propelinear codes

Let S_n denote the symmetric group of permutations of the set $\{1,2,\dots,n\}$. For any $\pi \in S_n$ and $v \in \mathbb{F}_2^n$, we denote by $(v_{\pi^{-1}(1)}, v_{\pi^{-1}(2)}, \dots, v_{\pi^{-1}(n)})$ the image of the vector $v = (v_1, v_2, \dots, v_n)$ by the permutation π.

Definition 1. *[2] A binary code C of length n has a **propelinear** structure if for each codeword $x \in C$ there exists $\pi_x \in S_n$ satisfying the following conditions:*

For all $x,y \in C$, $x + \pi_x(y) \in C$ and $\pi_x\pi_y = \pi_z$, where $z = x + \pi_x(y)$.

For all $x \in C$ and for all $y \in \mathbb{Z}_2^n$, denote by $*$ the binary operation such that $x * y = x + \pi_x(y)$. Then, $(C,*)$ is a group, which is not abelian in general. The vector $\mathbf{0}$ is always a codeword and $\pi_{\mathbf{0}}$ is the identity permutation. Hence, $\mathbf{0}$ is the identity element in C and $x^{-1} = \pi_{x^{-1}}(x)$, for all $x \in C$, [2]. We call C an Hadamard propelinear code if it has a propelinear structure and it is an Hadamard code.

As an example, let Q_8 be the group of quaternions which can be presented as $Q_8 = \{\mathbf{a}, \mathbf{b} : \mathbf{a}^4 = \mathbf{e}; \mathbf{a}^2 = \mathbf{b}^2 = \mathbf{u}, \mathbf{bab}^{-1} = \mathbf{a}^{-1}\} = \{\mathbf{e}, \mathbf{a}, \mathbf{a}^2, \mathbf{a}^3, \mathbf{b}, \mathbf{ab}, \mathbf{a}^2\mathbf{b}, \mathbf{a}^3\mathbf{b}\}$. We use the *Gray map* given by $\mathbf{e} \to (0,0,0,0)$, $\mathbf{b} \to (0,1,1,0)$, $\mathbf{a} \to (0,1,0,1)$, $\mathbf{ab} \to (1,1,0,0)$, $\mathbf{a}^2 \to (1,1,1,1)$, $\mathbf{a}^2\mathbf{b} \to (1,0,0,1)$, $\mathbf{a}^3 \to (1,0,1,0)$, $\mathbf{a}^3\mathbf{b} \to (0,0,1,1)$. As a propelinear code, the associated permutations to the generator elements of Q_8 are: $\pi_{\mathbf{a}} = (1,2)(3,4)$, $\pi_{\mathbf{b}} = (1,3)(2,4)$. From now on, we use $\mathbf{e}$ for the binary all-zero vector and $\mathbf{u}$ for the binary all-one vector.

Definition 2. *An Hadamard full propelinear code is an Hadamard propelinear code C such that for every $a \in C$, $a = \mathbf{e}$, $a = \mathbf{u}$, the permutation π_a has not any fixed coordinate and $\pi_{\mathbf{e}} = \pi_{\mathbf{u}} = I$. From now on, we denote by* HFP*-codes the Hadamard full propelinear codes.*

Ito proved in [6] that there is no Hadamard group realizing a dihedral group neither a cyclic group C_{8n}, and conjectured that for any length we can construct an Hadamard group of type Q, so a dicyclic group or a $C_n \rtimes Q_8$. Ryser [11] conjectured that there is no an Hadamard circulant matrix of length $8n$, which corresponds to a $C_{4n} \times C_2$ propelinear structure. Along the non-abelian groups of order $8n$, we focused our interest in Hadamard codes realizing a $C_n \times Q_8$ group structure.

3 HFP-codes of type C_nQ_8, n odd

Hadamard codes C of type C_nQ_8 were partially studied by Baliga and Horadam in [1]. In the current paper we study the minimum number of generators of C, we compute the rank and the dimension of the kernel and, finally, we give an example of such HFP-codes.

Definition 3. *Let C be an* HFP*-code of length $4n$. We say that C is a code of type C_nQ_8 when C is the direct product $C_n \times Q_8$.*

Lemma 4. *Let $C = \langle a, b, c\rangle$ be an* HFP*-code of type C_nQ_8, with n odd Then $C = \langle d, b\rangle$, where $d = ac$. Further, knowing d we can define b, uniquely (up to complementary).*

Proposition 5. *Let C be an* HFP*-code of type C_nQ_8 and length $4n$. Up to equivalence, we can fix the value of permutations associated to the elements of C. Further, the group generated by the associated permutations to each element of C is*

$$\Pi = C/\langle \mathbf{u}\rangle = C_2^2 \times C_n.$$

Proposition 6. *Let C be an* HFP*-code of type C_nQ_8 with n odd. Then, the rank of C is $r = 4n-1$ and the dimension of the kernel is $k = 1$.*

Now, we present an example of an HFP-code of type C_3Q_8.

Example 7. *Let $Q_8 = \langle a, b \mid a^4 = \mathbf{e}, a^2 = b^2 = \mathbf{u}, ab = ba^{-1}\rangle$ and $C_3 = \langle c \mid c^3 = \mathbf{e}\rangle$. We can take $a, b, c \in \mathbb{Z}_2^{12}$ with associated permutations as*

$$\begin{aligned}
a = &\ (0,1,1,1,0,0,0,1,0,1,0,1),\ \pi_a = (1,4)(2,5)(3,6)(7,10)(8,11)(9,12),\\
b = &\ (0,1,1,1,0,1,1,0,0,0,1,0),\ \pi_b = (1,7)(2,8)(3,9)(4,10)(5,11)(6,12),\\
c = &\ (0,0,0,1,0,1,1,0,1,1,0,1),\ \pi_c = (1,5,3)(2,6,4)(7,11,9)(8,12,10).
\end{aligned}$$

Then $C = \langle a, b, c\rangle$ is an HFP*-code of type $C_3 \times Q_8$ and $\Pi = \langle \pi_a, \pi_b, \pi_c\rangle = C_2^2 \times C_3$.*

4 HFP-codes of type C_nQ_8, n even

A standard method to construct Hadamard matrices from other Hadamard matrices is given by the the Kronecker product construction, [9]. Here, we adapt the Kronecker product, that we call *Kronecker sum construction*, and starting from an HFP-code of type C_nQ_8, n odd, we obtain HFP-codes of type $C_{2n}Q_8$ and $C_{4n}Q_8$.

Proposition 8. *Let $A = (a_{ij}), B = (b_{ij})$ be Hadamard matrices corresponding to* HFP*-codes of length m, n, respectively, then the code with corresponding matrix given by (1) is an* HFP*-code.*

$$A \oplus B = \begin{pmatrix} a_{11}+B & a_{12}+B & \cdots & a_{1m}+B \\ a_{21}+B & a_{22}+B & \cdots & a_{2m}+B \\ \vdots & \vdots & \vdots & \vdots \\ a_{2m,1}+B & a_{2m,2}+B & \cdots & a_{2m,m}+B \end{pmatrix} \tag{1}$$

Let $S = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ be the Hadamard matrix of length 2, and C_S the corresponding Hadamard code, which is an HFP-code, $C_S = \{(0,0),(0,1)),(1,0),(1,1)\}$, with associated permutations $\pi_{(0,0)} = \pi_{(1,1)} = I$, $\pi_{(1,0)} = \pi_{(0,1)} = (1,2)$. Consider also, the propelinear Hadamard code C_T of length 4 with associated matrix given by

$$T = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

and with associated permutations $\pi_{0000} = I$, $\pi_{1001} = (1234)$, $\pi_{0101} = (13)(24)$, $\pi_{0011} = (1432)$. Note that matrix T is equivalent to the unique circulant matrix of order 4 and code C_T is an HFP-code.

Proposition 9. *Let C be an* HFP*-code of type C_nQ_8 and length* $4n$*, n odd. Let A be the corresponding Hadamard matrix, so $C = C_A$. Then,*

i) We can define a propelinear structure in $C_{S\oplus A}$ resulting in an HFP*-code of type $C_{2n}Q_8$. The values of the rank and dimension of the kernel for this code are* $4n$ *and* 2*, respectively.*

ii) $C_{T\oplus A}$ is an HFP*-code of type $C_{4n}Q_8$. The values of the rank and dimension of the kernel for this code are* $4n+1$ *and* 3*, respectively.*

Note that we can not octuplicate C with the same technique as in Proposition 9. To do that we need an Hadamard matrix like T, but of order eight. This goes against the circulant Hadamard conjecture [11]. This consideration leads to consider the existence of HFP-codes of type $C_{2^sn}Q_8$ as an open problem, for $s \geq 3$ and n odd.

5 Acknowledgement

This work has been partially supported by the Spanish MICINN grant TIN2013-40524 and the Catalan AGAUR grant 2014SGR-691.

References

[1] A. Baliga and K. J. Horadam *Cocyclic Hadamard matrices over $\mathbb{Z}_n \times \mathbb{Z}_2^2$*, Australasian Journal of Combinatorics, **11**, pp.123-134, 1995.

[2] J. Basart, L. Huguet and J. Rifà. *On completely regular propelinear codes*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, pp. 341-355, 1989.

[3] A. del Río and J. Rifà. *Families of Hadamard $\mathbb{Z}_2\mathbb{Z}_4Q_8$-Codes,* IEEE Transactions on Information Theory, **59**, 8, pp. 5140-5151, 2013.

[4] W. de Launey, D.L. Flannery and K.J. Horadam. *Cocyclic Hadamard matrices and difference sets*, Discrete Applied Mathematics **102**, pp. 47-61, 2000.

[5] N. Ito. *On Hadamard Groups,* Journal of Algebra, **3**, 168, pp. 981-987, 1994.

[6] N. Ito. *On Hadamard groups III*, Kyushu Journal of Mathematics, **51**, 2, pp. 369-379, 1997.

[7] D.L. Flannery. *Cocyclic Hadamard matrices and Hadamard groups are equivalent*, J. Algebra **192**, pp. 749-779, 1997.

[8] P. Montolio, and J. Rifà. *Construction of Hadamard-Codes for Each Allowable Value of the Rank and Dimension of the Kernel.* Information Theory, IEEE Transactions, textbf61.4, pp. 1948-1958, 2015.

[9] K. Phelps, J. Rifà and M.Villanueva. *Hadamard Codes of Length 2^ts (s Odd). Rank and Kernel*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, pp. 328-337, 2006.

[10] J. Rifà, E. Suárez. *About a class of Hadamard propelinear codes,* Electronic Notes in Discrete Mathematics, **46**, pp.289-296, 2014.

[11] J. H. Ryser. *Combinatorial Mathematics, volume 14 of The Carus Mathematical Monographs*, The Mathematical Association of America, **342** , 1963.

A Message Encryption Scheme Using Idempotent Semirings

M. Durcheva

Technical University of Sofia, Bulgaria, mdurcheva66@gmail.com

Symmetric-key and public-key encryption have a number of complementary advantages. Symmetric key cryptography is faster and more efficient than asymmetric (public key) cryptography, but it lacks security when exchanging keys over unsecured channels. Furthermore, in symmetric key cryptography sound cryptographic practice dictates that the key be changed frequently whereas in public key cryptography a private key/public key pair may remain unchanged for considerable periods of time (see [3]).

In the present work a message encryption scheme based on public key establishment is proposed. For key exchanging phase we suggest using idempotent semirings [1, 2].

References

[1] M. Durcheva, *Public Key Cryptosystem Based on Two Sided Action of Different Exotic Semirings*, in Journal of Mathematics and System Science 4, pp. 6-13 (2014).

[2] M. Durcheva, *An application of different dioids in public key cryptography*, in AIP Conference Proceedings 1631, pp. 336-343 (2014).

[3] A. Menezes, P. vanOorschot and S. Vanstone *Handbook of Applied Cryptography*, CRC Press (1996).

Simplicial topological coding and homology of spin networks

V. Berec[1,2]

[1] *Institute of Nuclear Sciences Vinca, Belgrade, Serbia, vberec@vinca.rs*
[2] *University of Belgrade, Belgrade, Serbia, bervesnai@gmail.com*

We study the commutation of the stabilizer generators embedded in the q-representation of higher dimensional simplicial complex. The specific geometric structure and topological characterization of 1-simplex connectivity is generalized to higher dimensional structure of ordered complex in the combinatorial Laplacian matrix defined on a closed compact surface. Obtained results of a consistent homology-chain basis are used to define connectivity and dynamical self organization of spin network system using quantum Monte Carlo simulation of continuous sequences of simplicial maps.

References

[1] A. Hatcher, *Algebraic Topology*, Cambridge, England: Cambridge University Press, (2002).

[2] V. Berec, *Phase space dynamics and control of the quantum particles associated to hypergraph states*,arXiv preprint arXiv:1411.4059, (2014).

[3] P. J. Pemberton-Ross, A. Kay, *Perfect quantum routing in regular spin networks*, Phys. Rev. Lett. 106(2), 020503, (2011).

Code-Based Cryptosystems Using Generalized Concatenated Codes

Karim Ishak, Sven Müelich, Sven Puchinger, Martin Bossert

Ulm University, Germany,
{karim.ishak, sven.mueelich, sven.puchinger, martin.bossert}@uni-ulm.de

Public-key cryptosystems nowadays are mostly based on number theoretic problems like factorization (RSA) and the discrete logarithm problem (Elgamal). However, such systems can be broken with quantum computers by applying Shor's algorithms [1] for solving both problems, factorization and discrete logarithm, in polynomial time. Hence there is a need for post-quantum cryptography, i.e., methods resisting quantum computers. Code-based cryptography, introduced by McEliece in 1978 [2], is one of these candidates. In the original work, the McEliece cryptosystem uses Goppa codes. Ongoing research work is investigating other classes of codes for use in this cryptosystem.

Code-based cryptosystems based on Ordinary Concatenated (OC) codes were suggested by Nicolas Sendrier in [3]. OC codes are characterized by a lower decoding complexity than non-concatenated codes. However, in order to reach the same level of security as the original cryptosystem, systems based on OC codes require larger key sizes than the ones based on Goppa codes. Generalized Concatenated (GC) codes also have the advantage of low decoding complexity at the cost of possessing larger key sizes. As explained in [4], comparing a GC and an OC code with the same number of codewords, a GC code has a larger minimum distance. On the other hand, when they both have the same minimum distance, a GC code has more codewords.

In [3, 5], it is shown that the structure of a randomly permuted OC code could be discovered. A cryptosystem using OC codes, can then be attacked through obtaining the structure of the inner and outer codes from the public generator matrix. The attack consists of three main steps. The first step is based on identifying the positions of the inner code blocks. The second step orders the positions of the elements of the inner code blocks with respect to each other. Finally, in the third step, a generator matrix for an equivalent inner code is obtained. Moreover, a generator matrix of a π-equivalent outer code is also obtained, where π symbolizes the Frobenius field automorphism and also any power of π results in a field automorphism. After obtaining the structures of the inner and outer codes, already known attacks could be applied to each of them in order to break the whole system.

In this work, code-based cryptosystems using GC codes are analyzed in light of Sendrier's attack [3, 5]. If a GC code could be converted to an OC code, the attack would be directly applicable. However, it is mentioned in [6] that this conversion in general leads to a nonlinear outer code of the OC code. We show that this conversion always leads to a nonlinear outer code of the OC code if the outer codes of the GC code are not all exactly the same, i.e, do not contain the same set of codewords.

Sendrier's attack is only partially applicable in a direct way to systems using GC codes. The first part of the attack can be applied just as for the case of OC codes but with corresponding conditions for the case of GC codes. The second step of the attack also works straightforwardly. A generator matrix of an equivalent inner code could also be obtained. However, the part of the third step of the attack, which is responsible for obtaining a π-equivalent outer code, is not directly applicable. We present a non-structural alternative to this third step that works for both OC and GC codes. Its applicability is based on the corresponding work factor. For the code parameters suggested by Sendrier in [3], the attack results in a work factor that is considered to be insecure. This attack is applied after the first and second steps of Sendrier's attack and after obtaining the generator matrix of an equivalent inner code. It is non-structural because it does not obtain a certain structure for the outer code. However, it is able to reconstruct the message. This non-structural attack is mainly based on the information set decoding attack which is mentioned in [2].

Sendrier's attack on cryptosystems using GC codes is restricted to certain constraints, similar to OC codes. We investigate the possibilities of choosing GC codes that might resist the attack, e.g., when the dual distance of the inner code is greater than or equal to the minimum of the minimum distances of the outer codes. In this case, the first step of Sendrier's attack is not guaranteed to work. Our work aims to provide an idea which GC codes might be suited for McEliece cryptosystems.

References

[1] Peter W. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*, 35th Annual Symposium on Foundations of Computer Science, 1994 Proceedings. pp. 124–134, IEEE (1994).

[2] Robert J. McEliece, *A Public-Key Cryptosystem Based On Algebraic Coding Theory*, DSN progress report. 42(44), pp. 114-116 (1978).

[3] Nicolas Sendrier, *On the Structure of Randomly Permuted Concatenated Code*, research report, RR-2460 <inria-00074216> (1995).

[4] Martin Bossert, *Channel Coding for Telecommunications*, John Wiley & Sons, Inc. (1999).

[5] Nicolas Sendrier, *On the Concatenated Structure of a Linear Code*, Applicable Algebra in Engineering, Communication and Computing. 9(3), pp. 221-242, Springer (1998).

[6] Hervé Chabanne and Nicolas Sendrier, *On the concatenated structures of a [49, 18, 12] binary abelian code*, Discrete mathematics. 112(1), pp. 245-248, Elsevier (1993).

Nearly Sparse Linear Algebra
and application to the Discrete Logarithm Problem

A. Joux[1], C. Pierrot[2]

[1] *CryptoExperts and Chaire de Cryptologie de la Fondation de l'UPMC, antoine.joux@m4x.org*
[2] *CNRS, DGA, and Sorbonne Universités, LIP6/UPMC, Paris, France, Cecile.Pierrot@lip6.fr*

In this talk, we propose a method to perform linear algebra on a matrix with nearly sparse properties. More precisely, although we require the main part of the matrix to be sparse, we allow some dense columns with possibly large coefficients. We modify Block Wiedemann algorithm and show that the contribution of these heavy columns can be made negligible compared to the one of the sparse part of the matrix. In particular, this eases the computation of discrete logarithms in medium and high characteristic finite fields, where *nearly sparse matrices* naturally appear.

Sparse Linear Algebra. Linear algebra is a widely used tool in both mathematics and computer science. At the boundary of these two disciplines, cryptography is no exception to this rule. Yet, one notable difference is that cryptographers mostly consider linear algebra over finite fields, bringing both drawbacks – the notion of convergence is no longer available – and advantages – no stability problems can occur. As in combinatory analysis or in the course of solving partial differential equations, cryptography also presents the specificity of frequently dealing with sparse matrices.

A sparse matrix is a matrix containing a relatively small number of coefficients that are not equal to zero. It often takes the form of a matrix in which each row (or column) only has a small number of non-zero entries, compared to the dimension of the matrix. With sparse matrices, it is possible to represent in computer memory much larger matrices, by giving for each row (or column) the list of positions containing a non-zero coefficient, together with its value. When dealing with a sparse linear system of equations, using plain Gaussian Elimination is often a bad idea, since it does not consider nor preserve the sparsity of the input matrix. Indeed, each pivoting step during Gaussian Elimination increases the number of entries in the matrix and, after a relatively small number of steps, it overflows the available memory.

Three families of sparse linear algebra algorithms. In order to deal with sparse systems, a different approach is required. Three main families of algorithms have been devised: the first one adapts the ordinary Gaussian Elimination in order to choose pivots that minimize the loss of sparsity and is generally used to reduce the initial problem to a smaller slightly less sparse problem. The two other algorithm families work in a totally different way. Namely, they do not try to modify the input matrix but aim at directly finding a solution of the sparse linear system by computing only matrix-by-vector multiplications. One of these families consists of Krylov Subspace methods, adapted from numerical analysis, and constructs sequences of mutually orthogonal vectors.

Block Wiedemann algorithm. Throughout this talk, we focus on the third family that contains Wiedemann algorithm and its generalizations. Instead of computing an orthogonal family of vectors, Wiedemann proposed in 1986 [5] to reconstruct the minimal polynomial of the considered matrix. This algorithm computes a sequence of scalars of the form ${}^twA^iv$ where v and w are two vectors and A the sparse matrix of the linear algebra problem. It tries then to extract a recursive relationship that holds for this sequence. Coppersmith and Kaltofen [2, 3] adapted Wiedemann algorithm for parallelization and even distributed computations. The main idea of Coppersmith's Block Wiedemann algorithm is to compute a sequence of matrices of the form ${}^tWA^iV$ where V and W are not vectors as previously but *blocks* of vectors. This step is parallelized by distributing the vectors of the block V to **several processors or CPUs – let us say** c. The asymptotic complexity of extracting the recursive relationships within the sequence of small matrices is in $\tilde{O}(cN^2)$ where N **is the largest dimension of the input matrix**. Finally, a further improvement was proposed by Thomé [4] in 2002: he reduced the complexity of finding the recursive relationships to $\tilde{O}(c^2N)$.

Note that both Krylov Subspace methods and Wiedemann algorithms cost a number of matrix-by-vector multiplications equal to a small multiple of the matrix dimension: for **a matrix containing λ entries per row in average**, the cost of these matrix-by-vector multiplications is $O(\lambda N^2)$. With Block Wiedemann, it is possible to distribute the cost of these products on c machines. In this case, the search for recursive relationships adds an extra cost of the form $\tilde{O}(c^2N)$.

Nearly Sparse Linear Algebra. For a *d-nearly sparse matrix*, which includes d dense columns in addition to its sparse part, the cost of matrix-by-vector multiplications increases. As a consequence, the total complexity becomes:

$$O((\lambda+d)N^2)+\tilde{O}(c^2N) \tag{1}$$

where the second term is an extra cost for Block Wiedemann.

In this talk, we present an algorithm to solve linear algebra problems associated to these special matrices. Our aim is to adapt the Coppersmith's Block Wiedemann algorithm to improve the cost of linear algebra on matrices that have nearly sparse properties and reduce it to:

$$O(\lambda N^2) + \tilde{O}(\max(c,d)^2 N). \tag{2}$$

We compare our method with preexisting linear algebra techniques and show that it is competitive even with a large number of dense columns. In particular, when the number of dense columns is lower than the number of processors we use for the matrix-by-vector steps, we show that the presence of these unwelcome columns does not affect the complexity of solving linear systems associated to these matrices.

Application to Discrete Logarithm Computations in Finite Fields. In practice, this result precisely applies to the discrete logarithm problem. Indeed, nearly sparse matrices appear in both medium and high characteristic finite fields discrete logarithm computations. To illustrate this claim, we recall the latest record [1] announced in June 2014 for the computation of discrete logarithms in a prime field GF_p, where p is a 180 digit prime number. It uses a matrix containing 7.28M rows and columns with an average weight of 150 non-zero coefficients per row and also presents 4 dense Schirokauer maps columns. These columns precisely give to the matrix the nearly sparse structure we study.

References

[1] Cyril Bouvier and Pierrick Gaudry and Laurent Imbert and Hamza Jeljeli and Emmanuel Thomé, *Discrete logarithms in GF(p) – 180 digits*, Announcement to the NMBRTHRY list, item 003161 (June 2014).

[2] Don Coppersmith, *Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm*, in Mathematics of Computation, **62**, pp. 333–350 (1994).

[3] Erich Kaltofen, *Analysis of Coppersmith's Block Wiedemann Algorithm for the Parallel Solution of Sparse Linear Systems*, in Mathematics of Computation, pp. 777–806 (1995).

[4] Emmanuel Thomé, *Subquadratic Computation of Vector Generating Polynomials and Improvement of the Block Wiedemann Algorithm*, in *J. Symb. Comput.* **33**, 5, pp. 757–775 (2002).

[5] Douglas H. Wiedemann, *Solving sparse linear equations over finite fields*, IEEE Transactions on Information Theory **32**, 1, pp. 54–62 (1986).

Computational Differential and Difference Algebra

Session Organizers

Carlos E. Arreche
Department of Mathematics
North Carolina State University
`cearrech@math.ncsu.edu`

Alexey Ovchinnikov
Department of Mathematics
City University of New York, Queens College
`aovchinnikov@qc.cuny.edu`

Michael Wibmer
Lehrstuhl für Mathematik
RWTH Aachen
`michael.wibmer@matha.rwth-aachen.de`

Overview

- Differential and difference Galois theories of linear differential and difference equations (with parameters)
- Applications to differential and difference algebraic dependencies among solutions of differential and difference equations
- Differential and difference elimination
- Interactions with computational aspects of differential and difference equations
- Interactions with traditional areas of symbolic computation
- Applications of differential and difference algebra

Root Parametrized Differential Equations for the Classical Groups

Matthias Seiß

Universität Kassel, Germany, matthias.seiss@mathematik.uni-kassel.de

This talk is about the inverse problem in differential Galois theory over the differential field $C\langle t_1,\ldots,t_l\rangle$, where C is an algebraic closed field of characteristic zero and $\boldsymbol{t}=(t_1,\ldots,t_l)$ are l differential indeterminates. For the differential ground field $C(z)$, i.e. the field of rational functions with standard derivation $\partial=\frac{d}{dz}$, it is well known that every linear algebraic group G defined over C occurs as a differential Galois group. In [3], C. Mitschi and M. Singer used bound criteria for the differential Galois group in this setting to construct very specific linear differential equations for connected semisimple linear algebraic groups. In this talk we transfer their results from $C(z)$ to the differential field $C\langle t_1,\ldots,t_l\rangle$ via specializations $\sigma: C\langle t_1,\ldots,t_l\rangle\to C(z)$. More precisely, we develop a lower bound criterion for the differential Galois group $G(C)$ of a matrix parameter differential equation $\partial(\boldsymbol{y})=A(\boldsymbol{t})\boldsymbol{y}$ over $C\langle t_1,\ldots,t_l\rangle$. We prove that the differential Galois group of the specialized equation $\partial(\boldsymbol{y})=A(\sigma(\boldsymbol{t}))\boldsymbol{y}$ is a subgroup of the differential Galois group of the original equation. Combing our bound criterion with the results of [3] we show that for every semisimple linear algebraic group of Lie rank l there exists an explicit linear parameter differential equation in l parameters, i.e. a differential equation of shape

$$y^{(n)}-\sum_{i=0}^{n-1}a_i(\boldsymbol{t})y^{(i)}=0 \text{ where } a_i(\boldsymbol{t})\in C\langle t_1,\ldots t_l\rangle. \tag{1}$$

As a second application we compute explicit and nice linear parameter differential equations over $C\langle t_1,\ldots,t_l\rangle$ for the groups $\mathrm{SL}_{l+1}(C)$, $\mathrm{SP}_{2l}(C)$, $\mathrm{SO}_{2l+1}(C)$, $\mathrm{SO}_{2l}(C)$, i.e. for the classical groups of type A_l, B_l, C_l, D_l, and for G_2 ($l=2$). For each group we explain how we choose the defining matrix $A(\boldsymbol{t})$ in the Lie algebra with respect to the root structure to obtain our equations: Given a root space decomposition we take for each simple root a constant non-zero matrix from its root space and we parametrize l root spaces which correspond to l specific negative roots each of height equal to one of the exponents of G. We use then results from [1], [2] to show that a large class of elements in the Lie algebra $g\otimes C(z)$ is gauge equivalent to specializations of $A(\boldsymbol{t})$.

In case of $\mathrm{SL}_{l+1}(C)$, we prove that our equations are generic in the following sense: If F is an algebraically closed differential field with constants C and E/F is a

Picard-Vessiot extension with differential Galois group $H(C) \subset \mathrm{SL}_{l+1}(C)$, then there exists a specialization of our equation which defines a Picard-Vessiot extension differentially isomorphic to E/F. Finally, we give explicit generators for the extensions defined by our differential equations.

References

[1] B. Kostant, *Lie Group Representations on Polynomial Rings*, Amer. J. Math., 85, (1963), 327-404.

[2] B. Kostant, *The Principal Three-Dimensional Subgroups and the Betti Numbers of a Complex Simple Lie Group*, Amer. Jour. of Math., 81, (1959), 973-1032.

[3] C. Mitschi and M.F. Singer, *Connected groups as differential Galois groups*, J. Algebra 184 (1996), 333-361.

Quasi-optimal computation of the p-curvature

A. Bostan[1], X. Caruso[2], É. Schost[3]

[1] *Inria, France, alin.bostan@inria.fr*
[2] *Université Rennes 1, France, xavier.caruso@normalesup.org*
[3] *Western University, London, Canada, eschost@uwo.ca*

The p-curvature of a system of linear differential equations in characteristic p is a matrix that measures to what extent the system is close to having a fundamental matrix of rational function solutions. We describe a recent algorithm [1] for computing the p-curvature. For a system of dimension r with rational function coefficients of degree at most d, its complexity is $\widetilde{O}(pdr^{\omega})$ operations in the ground field (where ω is the matrix multiplication exponent and the soft-O notation $\widetilde{O}$ hides polylogarithmic factors), whereas the size of the output is about pdr^2. Our algorithm is then quasi-optimal assuming that matrix multiplication is (*i.e.* $\omega = 2$). The design of the algorithm relies on the existence of a well-suited ring of series with divided powers for which an analogue of the Cauchy–Lipschitz Theorem holds.

References

[1] A. Bostan, X. Caruso and É. Schost, *A Fast Algorithm for Computing the p-Curvature*, in *Proc. ISSAC 2015*, ACM Press, 2015.

The Positive Part of Multivariate Series

A. Bostan[1], F. Chyzak[1], M. Kauers[2], L. Pech, M. van Hoeij[3].

[1] *INRIA Saclay Ile de France, France, {alin.bostan, frederic.chyzak}@inria.fr,*
[2] *Institute for Algebra, Johannes Kepler University, Linz, Austria, manuel.kauers@algebra.jku.at*
[3] *Department of Mathematics, Florida State University, USA, hoeij@math.fsu.edu*

For formal Laurent series in one variable, the positive part is defined as the formal power series which is obtained by discarding from the Laurent series all the terms with a negative exponent. In the talk, we shall discuss the case of several variables. Certain generating functions in combinatorics are shown to be D-finite by writing them as the positive part of some multivariate rational function. But it is not so obvious what this really means. We will present a general and formally sound interpretation which gives rise to a new way to construct the differential equations satisfied by the positive part of a multivariate rational function. This result arose in the context of classifying the generating functions of walks in the quarter plane (cf. my talk in the AADIOS session at this ACA). Details will appear in [2]. For the definition and fundamental properties of formal Laurent series in several variables, see [1].

References

[1] A. Aparicio Monforte and M. Kauers, *Multivariate Laurent Series in Several Variables*, Expositiones Mathematicae 31(4):350–367, Dec. 2013

[2] A. Bostan, F. Chyzak, M. Kauers, L. Pech, M. van Hoeij, *in preparation*

Prolongation spaces and generalized differentials

F. Heiderich[1]

[1] *National Research University Higher School of Economics, Moscow, Russian Federation*
fheiderich@hse.ru

The tangent bundle of an affine scheme can be described in terms of the module of Kähler differentials. The literature contains several definitions of prolongation spaces, which generalize the tangent bundle. We propose a definition of generalized differentials and show how they can be used to construct the above-mentioned prolongation spaces. Our construction is not limited to the "differential case", but applies also in the "difference case" and in more general contexts. In particular we obtain a concrete realization of the prolongation spaces that have been defined recently by Moosa and Scanlon.

Unitary groups of group algebras in characteristic 2

M. Barakat[1]

[1] *RWTH Aachen University, Germany, {mohamed.barakat}@rwth-aachen.de*

The following problem was posed by J.-P. Serre:
Consider the group algebra kG of a finite group G over an algebraically closed field k of characteristic 2. Denote by $U_G := U_{kG}$ the unitary group of kG quipped with its standard involution generated by $g \mapsto g^{-1}$. Serre was particularly interested in determining the group of components $\pi_0(U_{A_5})$, where A_5 is the alternating group on five points. Combining Singular and GAP the triviality of $\pi_0(U_{A_5})$ could be proven. Further systematic computations reveal an interesting pattern for $\pi_0(U_G)$. This pattern starts emerge at group orders where hand computations become virtually impossible.

On the computation of the difference-differential Galois group for a second-order linear difference equation

C.E. Arreche[1]

[1] *North Carolina State University, USA {cearrech}@math.ncsu.edu*

Given a linear difference equation, there is a difference-differential Galois group that encodes the differential-algebraic dependencies among the solutions of the equation. I will describe algorithms to compute the Galois group associated to a second-order linear difference equation over $\mathbf{C}(x)$, the field of rational functions over the complex numbers, with respect to the shift automorphism that sends x to $x+1$. I will also discuss some concrete examples to illustrate these algorithms.

References

[1] C. Hardouin and M.F. Singer, *Differential Galois theory of linear difference equations*, Math. Ann. **342**, pp. 333–377 (2008).

[2] P.A. Hendriks, *An algorithm determining the difference Galois group of second order linear difference equations*, J. Symbolic Computation **26**, pp. 445–461 (1998).

[3] M. van der Put and M.F. Singer, *Galois theory of difference equations*, Lecture Notes in Mathematics, vol. 1666. Springer, Heidelberg (1997).

Differential Galois theory over differentially simple rings

A. Maurischat[1]

[1] *Goethe University Frankfurt, Germany, maurisch@math.uni-frankfurt.de*

Considering fields as commutative rings having only (0) and (1) as ideals, their analogs in the differential setting are differentially simple rings. It is therefore natural to ask whether their exists a differential Galois theory of differentially simple rings rather than of differential fields. In this talk, we present a positive answer to that question which is worked out in [1] in more detail. We also give an example of a non-free differential module over a differentially simple ring, and compute the corresponding Picard-Vessiot ring.

References

[1] A. Maurischat, *Picard-Vessiot theory of differentially simple rings*, Journal of Algebra **409**, pp. 162-181 (2014).

Malher equations, differential Galois theory, and transcendence

T. Dreyfus[1], C. Hardouin[2], J. Roques[3]

[1] *University of Toulouse, France, thomas.dreyfus@ens-cachan.org*
[2] *University of Toulouse, France, hardouin@math.univ-toulouse.fr*
[3] *University of Grenoble, France, Julien.Roques@ujf-grenoble.fr*

This is a joint work with C. Hardouin and J. Roques. Malher equations are equations involving the operator $\phi_p f(z) := f(z^p)$. Generating series of p-exacte sentence are naturally solution of Malher equations.

Nishioka has given necessary and sufficient condition on $a, b \in C(z)$, to determine whether a solution of $\phi_p y = ay + b$ is hyper-transcendental or not. In this talk, we are going to explain how the parametrized differential Galois theory developed by Hardouin and Singer will help us to give necessary and sufficient condition on $a, b \in C(z)$, to determine whether the solutions of $\phi_p^2 y = a\phi_p y + by$ are hyper-transcendental or not.

Primitive recursive quantifier elimination for existentially closed difference fields

I. Tomašić[1]

[1] *Queen Mary University of London, UK,* i.tomasic@qmul.ac.uk

Chevalley's theorem states that the image of a morphism of algebraic varieties over an algebraically closed fields is constructible. This is equivalent to Tarski's theorem that the theory of algebraically closed fields admits quantifier elimination. This talk will discuss our solution to the problem of images of morphisms of difference varieties over existentially closed difference fields.

It was known since [2] and [1] that the class of existentially closed difference fields is axiomatisable in first-order logic by the theory called ACFA. This theory does not eliminate quantifiers in the language of rings, so in order to consider images of morphisms of difference varieties, one needs to consider formulae with a single (bounded) existential quantifier.

Consequently, ACFA is decidable, but the classical elimination/decision algorithm stems from the use of compactness and completeness theorems of first-order logic and therefore proceeds via unbounded searches through the list of all suitable existential formulae and, for each one, through all candidate proofs of either its equivalence or non-equivalence to the original formula.

Our work on *Galois stratification* in difference algebraic geometry yields the following improvements.

1. In [5] and [4], we establish a *finer description* of first-order formulae in ACFA in terms of *Galois covers* of difference varieties, and prove that the resulting quantifier elimination is primitive recursive reducible to a few algorithms in difference algebra. Such algebraic-geometric description of formulae is suitable for a variety of number-theoretic applications.

2. In [3], we develop the Galois stratification formalism in the context of *directly presented* difference varieties. The resulting quantifier elimination is equivalent to the logic one, but our elimination procedure is *primitive recursive*.

We will give an overview of these results from the point of view of computability in difference algebra.

References

[1] Zoé Chatzidakis and Ehud Hrushovski. Model theory of difference fields. *Trans. Amer. Math. Soc.*, 351(8):2997–3071, 1999.

[2] Angus Macintyre. Generic automorphisms of fields. *Ann. Pure Appl. Logic*, 88(2-3):165–180, 1997.

[3] Ivan Tomašić. Direct twisted Galois stratification. `arXiv:1412.8066`, 2014. Submitted.

[4] Ivan Tomašić. Galois stratification and ACFA. *Ann. Pure Appl. Logic*, 166(2015), no. 5, 639–663.

[5] Ivan Tomašić. Twisted Galois stratification. `arXiv:1112.0802`, 2012. To appear in *Nagoya Mathematical Journal*.

Lagrangian Constraints and Differential Thomas Decomposition

V. P. Gerdt[1], D. Robertz[2]

[1] *Laboratory of Computing Techniques and Automation, Joint Institute for Nuclear Research, 141980 Dubna, Russia, gerdt@jinr.ru*
[2] *Centre for Mathematical Sciences, Plymouth University, 2-5 Kirkby Place, Drake Circus, Plymouth PL4 8AA, UK, daniel.robertz@plymouth.ac.uk*

Most of the fundamental laws of physics can be described in a field-theoretical framework by an action, which is an integral of a Lagrangian density. The principle of least action yields Euler-Lagrange equations. It is an important problem to compute the constraints which follow from the Euler-Lagrange equations. If the Lagrangian model is given by differential polynomials, we show that Thomas decomposition is an algorithmic tool for the computation of Lagrangian constraints. We present differential elimination techniques which are relevant for this purpose. The Thomas decomposition method has been implemented in Maple packages by T. Bächler and M. Lange-Hegermann.

References

[1] T. Bächler and M. Lange-Hegermann, `AlgebraicThomas` *and* `DifferentialThomas`*: Thomas decomposition of algebraic and differential systems*, freely available at `http://wwwb.math.rwth-aachen.de/thomasdecomposition`, 2008–2014.

[2] V. P. Gerdt and D. Robertz, *Lagrangian Constraints and Differential Thomas Decomposition*, submitted for publication.

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

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

[5] A. Wipf, *Hamilton's formalism for systems with constraints*, in: J. Ehlers and H. Friedrich (eds.), Canonical gravity: from classical to quantum (Bad Honnef, 1993), vol. 434 of Lecture Notes in Physics, Springer, Berlin, 22–58, 1994 (arXiv:hep-th/9312078).

Geometric Singularities of Algebraic Differential Equations

Werner M. Seiler[1]

[1] *Institut für Mathematik, Universität Kassel, Germany, seiler@mathematik.uni-kassel.de*

Differential equations exhibit many kinds of singular phenomena. In this talk, we will discuss singularities of the equations themselves—which is something different than singularities of *solutions* of the equations. Our approach "interpolates" between three different domains. Within *differential algebra*, which here means mainly differential ideal theory [6, 7], the notion of singular integrals as solutions not contained in the general solution has played an important role (in fact, it was the problem that motivated Ritt to develop this theory). Within *differential topology*, singularities of differential equations represent a special case of the theory of singularities of smooth maps between manifolds [1, 3]. Here the main emphasis has been on complete classifications for scalar ordinary differential equations of lower order. In the context of *differential algebraic equations*, singularities of quasi-linear systems have been studied mainly by analytic methods [4, 5].

The talk will consist of three parts. In the first part, we develop a suitable notion of algebraic differential equations. As some of the techniques we will later apply assume that the underlying field is algebraically closed, we are dealing throughout with complex equations and holomorphic solutions. We then define algebraic differential equations as certain algebraic subsets of a jet bundle and introduce some algebraic and geometric structures on them. This leads then to a rigorous notion of a regular differential equation.

In the second part, we follow ideas from differential topology to define regular and irregular singular points for algebraic differential equations. In contrast to the literature, our definitions are valid for arbitrary systems of ordinary or partial differential equations. For systems which are not of finite type, this requires to consider a whole neighbourhood of the point. For scalar ordinary differential equations we will demonstrate with some simple examples the typical behaviour of solutions in the neighbourhood of such singularities.

In the last part, we will present an algorithm for the detection of all singularities of a differential equation at a prescribed order. The key tools for this algorithm are the algebraic and the differential Thomas decomposition [2, 8]. With the differential Thomas decomposition, the given system is decomposed in suitably "nice" systems. The differential ideal for each of these is then truncated at the prescribed order and a purely algebraic analysis of the obtained algebraic differential equation and some geometric structures on it is performed.

References

[1] V.I. Arnold, S.M. Gusejn-Zade, and A.N. Varchenko. *Singularities of Differentiable Maps I: The Classification of Critical Points, Caustics and Wave Fronts*. Monographs in Mathematics 82. Birkhäuser, Boston, 1985.

[2] T. Bächler, V.P. Gerdt, M. Lange-Hegermann, and D. Robertz. *Algorithmic Thomas decomposition of algebraic and differential systems*. J. Symb. Comp., 47:1233–1266, 2012.

[3] M. Golubitsky and V.W. Guillemin. *Stable Mappings and Their Singularities*. Graduate Texts in Mathematics 14. Springer-Verlag, New York, 1973.

[4] P.J. Rabier and W.C. Rheinboldt. *Theoretical and numerical analysis of differential-algebraic equations*. In P.G. Ciarlet and J.L. Lions, editors, Handbook of Numerical Analysis, volume VIII, pages 183–540. North-Holland, Amsterdam, 2002.

[5] R. Riaza. *Differential-Algebraic Systems*. World Scientific, Hackensack, 2008.

[6] J.F. Ritt. *Differential Equations from the Algebraic Standpoint*. Amer. Math. Soc., Providence (RI), 1932.

[7] J.F. Ritt. *Differential Algebra*. Dover, New York, 1966. (Original: AMS Colloquium Publications, Vol. XXXIII, 1950).

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

Symbolic Solution of First-Order Autonomous Algebraic Partial Differential Equations

F. Winkler[1]

[1] *Johannes Kepler Universität, Linz, Austria, franz.winkler@risc.jku.at*

Recently algebro-geometric solution methods for algebraic ordinary differential equations (AODEs) have been investigated. The starting point was an algorithm by Feng and Gao [1] which decides whether or not an autonomous AODE, $F(y,y') = 0$, has a rational solution and in the affirmative case computes a rational general solution. This result was then generalized by Ngô and Winkler [2] to the non-autonomous case $F(x,y,y') = 0$. In the algebro-geometric approach we first neglect the differential aspect of the problem, and consider the algebraic surface $\mathscr{S}$ defined by $F(x,y,z) = 0$. From a parametric representation of $\mathscr{S}$ we then decide solvability of the differential equation in a given class of functions, and in the affirmative case compute solutions.

A generalization of the procedure to algebraic partial differential equations (APDEs) in two variables can be found in [3]. Here we present a further generalization to the case of APDEs in an arbitrary number of variables.

For example, our method is able to compute the rational solution $\frac{x}{y}$ of the inviscid Burgers equation (see [4]) $uu_x + u_y = 0$, or the solution $\frac{\mathrm{e}^{-x\beta}\left(1-\mathrm{e}^{x\beta}\right)\alpha}{(1+\mathrm{e}^{\alpha y})\beta}$ of the (special case of the) generalized Burgers $u_y + uu_x + \alpha u + \beta u^2 = 0$.

This is joint research with G. Grasegger, A. Lastra, and J.R. Sendra.

References

[1] R. Feng and X.-S. Gao, *A polynomial time algorithm for finding rational general solutions of first order autonomouos ODEs*, J. Symbolic Computation **41**, pp. 739-762 (2006).

[2] L.X.C. Ngô and F. Winkler, *Rational general solutions of first order non-autonomous parametrizable ODEs*, J. Symbolic Computation **45/12**, pp. 1426-1441 (2010).

[3] G. Grasegger, A. Lastra, J.R. Sendra and F. Winkler, *On symbolic solutions of algebraic partial differential equations*, in V.P. Gerdt et al. (eds.), Proceedings of the 16th Workshop on Computer Algebra in Scientific Computing (CASC-2014), Springer LNCS 8660, pp. 111-120 (2014).

[4] D. Zwillinger, Handbook of Differential Equations, Academic Press, 3rd ed. (1998).

Algebraic and Algorithmic Differential and Integral Operator

Session Organizers

Moulay Barkatou
University of Limoges
moulay.barkatou@unilim.fr

Thomas Cluzeau
University of Limoges
thomas.cluzeau@unilim.fr

Georg Regensburger
Austrian Academy of Sciences
RICAM, Linz
georg.regensburger@oeaw.ac.at

Markus Rosenkranz
University of Kent
SMSAS, Canterbury
M.Rosenkranz@kent.ac.uk

Overview

The algebraic/symbolic treatment of differential equations is a flourishing field, branching out in a variety of subfields committed to different approaches. In this session, we want to give special emphasis to the operator perspective of both the underlying differential operators and various associated integral operators (e.g. as Green's operators for initial/boundary value problems).

Birational Transformations of Algebraic Ordinary Differential Equations

F. Winkler[1]

[1] *Johannes Kepler Universität, Linz, Austria, franz.winkler@risc.jku.at*

An algebraic ordinary differential equation (AODE) is a polynomial relation

$$F(x,y,y',\dots,y^{(n)})=0$$

between the unknown function y and its derivatives, possibly involving the variable of differentiation x, where F is a differential polynomial in $K[x]\{y\}$ with K being a differential field and the derivation $'$ being $\frac{d}{dx}$.

In the algebro-geometric approach we consider the algebraic hypersurface defined by the polynomial F. From a rational parametrization of this hypersurface, we can decide the rational solvability of the given AODE, and in fact compute the general rational solution. This approach has been developed for autonomous first order AODEs by Feng and Gao [1], and for non-autonomous first order AODEs by Ngô and Winkler [2].

Transforming the ambient space by some group of transformations, we get a classification of AODEs, such that equivalent equations share the property of rational solvability. The action of the group of affine transformations on AODEs has been investigated by Ngô, Sendra, and Winkler in [3]. Here we describe the action of the group of birational transformations.

For example, the first order AODE

$$F(x,y,y')=25x^2y'^2-50xyy'+25y^2+12y^4-76xy^3+168x^2y^2-144x^3y+32x^4=0$$

can be birationally transformed into the AODE $G(y,y')=y'^2-4y=0$. By the inverse transformation we derive from the rational general solution $y=(x+c)^2$ of $G(y,y')=0$ the rational general solution $y=\frac{x(2(x+c)^2+1)}{(x+c)^2+3}$ of $F(x,y,y')=0$.

This is joint research with L.X.C. Ngô and J.R. Sendra.

References

[1] R. Feng and X.-S. Gao, *A polynomial time algorithm for finding rational general solutions of first order autonomouos ODEs*, J. Symbolic Computation **41**, pp. 739-762 (2006).

[2] L.X.C. Ngô and F. Winkler, *Rational general solutions of first order non-autonomous parametrizable ODEs*, J. Symbolic Computation **45/12**, pp. 1426-1441 (2010).

[3] L.X.C. Ngô, J.R. Sendra and F. Winkler, *Classification of algebraic ODEs with respect to rational solvability*, Contemporary Mathematics **572**, pp. 193-210 (2012).

Controlled and conditioned invariance for polynomial and rational feedback systems

C. Schilli[1], E. Zerz[2], V. Levandovskyy[3]

[1] *RWTH Aachen University, Aachen, Germany, christian.schilli@math.rwth-aachen.de*
[2] *RWTH Aachen University, Aachen, Germany, eva.zerz@math.rwth-aachen.de*
[3] *RWTH Aachen University, Aachen, Germany, viktor.levandovskyy@math.rwth-aachen.de*

The investigation of invariant varieties for polynomial control systems leads to several algebraic intersection problems: Let K be a field. Given an ideal I of a commutative polynomial ring $R = K[x_1,\dots,x_n]$ and polynomials $\alpha, h_1,\dots,h_p \in R$, we want to find the intersection of the affine ideal $\alpha + I$ with the subalgebra of R generated by the h_i's; shortly, we want to determine the set

$$(\alpha + I) \cap K[h_1,\dots,h_p].$$

This will be the foundation for the following considerations: If Q is the quotient field of R and $d \in R$ is another polynomial, the set $\frac{1}{d} \cdot I \subseteq Q$ is a fractional ideal. Similar to the above, we are interested in finding the intersection of the affine fractional ideal $\alpha + \frac{1}{d} \cdot I$ with the subfield of Q generated by the h_i's:

$$(\alpha + \frac{1}{d} \cdot I) \cap K(h_1,\dots,h_p).$$

Using techniques from Gröbner basis theory, we will present methods to compute these intersections. For the second problem, we need to restrict to $p = 1$ and we will point out why the general setting seems more difficult. Further, we give definitions of controlled and conditioned invariant varieties in the control theoretical setting, and show how the methods from above can be applied to this framework.

References

[1] C. Schilli, E. Zerz and V. Levandovskyy, *Controlled and conditioned invariant varieties for polynomial control systems*, in Proceedings of the **21**st International Symposium on Mathematical Theory of Networks and Systems, University of Groningen, pp. 1691-1697 (2014).

[2] E. Zerz, S. Walcher, *Controlled invariant hypersurfaces of polynomial control systems*, Qualitative theory of dynamical systems **11**, pp. 145-158 (2012).

Invariant histograms and signatures for object recognition, symmetry detection, and jigsaw puzzle assembly

Peter J. Olver[1]

[1] *University of Minnesota, Minneapolis, MN, USA, olver@umn.edu*

I will survey recent developments in the use of differential invariant signatures for object recognition and symmetry detection in images, including applications to automated jigsaw puzzle assembly in both 2 and 3 dimensions.

References

[1] Calabi, E., Olver, P.J., Shakiban, C., Tannenbaum, A., and Haker, S., *Differential and numerically invariant signature curves applied to object recognition*, Int. J. Computer Vision **26** (1998) 107–135.

[2] Brinkman, D., and Olver, P.J., *Invariant histograms*, Amer. Math. Monthly **119** (2012) 4–24.

[3] Hoff, D., and Olver, P.J., *Extensions of invariant signatures for object recognition*, J. Math. Imaging Vision **45** (2013) 176–185.

[4] Hoff, D., Olver, P.J., *Automatic solution of jigsaw puzzles*, J. Math. Imaging Vision **49** (2014) 234–250.

[5] Grim, A., Olver, P.J., Shakiban, C., Slechta, R., and Thompson, R., *Automatic reassembly of three–dimensional jigsaw puzzles*, preprint, 2015.

Jacobi algebras, in-between Poisson, differential, and Lie algebras

L. Poinsot[1,2]

[1] *LIPN - CNRS (UMR 7030), University Paris 13, Sorbonne Paris Cité, France,*
laurent.poinsot@lipn.paris13.fr
[2] *CReA, French Air Force Academy, Base aérienne 701, France*

In the non-differential setting there is a functorial relation between Lie algebras and associative algebras: any algebra becomes a Lie algebra under the commutator bracket, and, conversely, to any Lie algebra is attached a universal associative envelope. In the realm of differential algebras, there are two such adjoint situations. The most obvious is obtained by lifting the above correspondence to differential algebras. At the contrary, the second connection is proper to the differential setting. Any commutative differential algebra admits the *Wronskian* bracket $xy' - x'y$ as a Lie bracket, and to any Lie algebra is provided a universal differential and commutative associative envelope.

A natural question is to know under which conditions a given Lie algebra embeds into its differential envelope. While an answer, for the non-differential setting, is known – the Poincaré-Birkhoff-Witt theorem – there are no yet any such solution in differential algebra. In a first part of this talk, after having briefly recalled the above construction, I will present some classes of Lie algebras for which the canonical map to their differential algebra is one-to-one.

Moreover, differential commutative algebras are merely not just Lie algebras, with help of their Wronskian bracket, but rather Lie-Rinehart algebras [2], the algebraic counterpart of a Lie algebroid.

However the Lie-Rinehart structure on a differential commutative algebra is just the consequence of a more abstract structure, namely that of a Jacobi algebra. A Jacobi algebra [1] is a commutative algebra A together with a Lie bracket $[-,-]$ (called *Jacobi bracket*) satisfying the following version of Leibniz rule:

$$[ab,c] = a[b,c] + b[a,c] - ab[1_A,c],\ a,b,c \in A.$$

A Jacobi bracket provides a derivation and an alternating biderivation. Hence forgetting one or the other of those differential operators provides a differential or a Poisson algebra, and these relations are functorial.

In a second part of the talk I will also present some of the functorial relations between Jacobi, differential, and Lie algebras, such as, e.g., the Jacobi envelope of a Lie algebra. I will also explain that the Lie algebra of global smooth sections of a line bundle E over a smooth manifold M (i.e., a vector bundle over M each fibre of which is one-dimensional) embeds, when E is trivial, into its Jacobi envelope.

References

[1] J. Grabowski, *Abstract Jacobi and Poisson structures. Quantization and star-products*, Journal of Geometry and Physics **9**, pp. 45-73 (1992).

[2] G. Rinehart, G., *Differential forms on general commutative algebras*, Trans. Amer. Math. Soc. **108**, pp. 195-222 (1963).

Quantized Weyl algebras and Automorphisms

A.Kitchin[1]

[1] *University of Kent, United Kingdom, ak562@kent.ac.uk*

In his foundational paper [4], Dixmier made the now famous conjecture: Every endomorphism of the Weyl algebra is an automorphism. Tsuchimoto, [7], and Belov-Kanel and Kontsevich, [3], proved independently that the Dixmier Conjecture is stably equivalent to the Jacobian Conjecture. It is natural to ask Dixmier's question for related algebras (see [2, 6]), and especially generalizations and quantizations of the Weyl algebras (see [1, 5]). Following this theme we introduce A_q, a quantization of the Weyl algebras, and prove a quantum analogue of the Dixmier conjecture: Every homomorphism of A_q is an automorphism.

This is joint work with Stéphane Launois.

References

[1] E. Backelin, *Endomorphisms of quantized Weyl algebras*, Lett. Math. Phys. 97 (2011), no. 3, 317-338.

[2] V. V. Bavula, *An analogue of the conjecture of Dixmier is true for the algebra of polynomial integro-differential operators*, J. Algebra 372 (2012), 237-250.

[3] A. Belov-Kanel and M. Kontsevich, *The Jacobian conjecture is stably equivalent to the Dixmier conjecture*, Mosc. Math. J. 7 (2007), no. 2, 209-218.

[4] J. Dixmier, *Sur les algèbres de Weyl*, Bull. Soc. Math. France 96 (1968), 209-242.

[5] G. Benkart, S.A. Lopes and M. Ondrus, *A parametric family of subalgebras of the Weyl algebra I. Structure and automorphisms.*, Trans. Amer. Math. Soc.367 (2015), no. 3.

[6] L. Richard, *Sur les endomorphismes des tores quantiques*, Comm. Algebra 30 (2002), no. 11, 5283-5306.

[7] Y. Tsuchimoto, *Preliminaries on Dixmier conjecture*, Mem. Fac. Sci. Kochi Univ. Ser. A Math. 24 (2003), 43-59.

On a generalization of integro-differential operators

Clemens G. Raab[1], Georg Regensburger[2]

[1] *RICAM, Austrian Academy of Sciences, Linz, Austria, clemens.raab@oeaw.ac.at*
[2] *RICAM, Austrian Academy of Sciences, Linz, Austria, georg.regensburger@oeaw.ac.at*

Algebras of differential and integral operators together with one or more evaluations (i.e. multiplicative functionals) have been studied and used a lot in recent years. We generalize the setting by also allowing non-multiplicative functionals. Such functionals arise naturally as generalized evaluation operators acting on functions with singularities, for example. Similarities and differences to the standard setting, in particular regarding identities and normal forms, will be discussed.

Application of Signature Curves to Characterize Melanomas and Moles

Cheri Shakiban[1], Anna Grim[2]

[1] *University of St. Thomas, St. Paul, Minnesota, USA {cshakiban@stthomas.edu}*

[2] *University of St. Thomas, St. Paul, Minnesota, USA {grim4684@stthomas.edu}*

Noninvasive diagnosis of melanoma persists as a challenge for dermatologists because of the structural differences between benign and malignant skin lesions are often indistinguishable to the human eye. This research focuses on the application of a 2D invariant curve, called the "signature curve", formed by taking curvature and derivative of curvature with respect to arc length of a closed curve: (κ, κ_s), [1, 2]. We can calculate the extended signature curves of the contours of the skin lesions [3] to detect asymmetry, border irregularity and diameter size of the skin lesions. In this paper, by analyzing the signature curves of 50 benign moles and 50 melanomas, we can show that the benign and malignant lesions have contrasting global and local symmetry patterns in their signature curves, [4]. Furthermore, regular moles are distinctive by a high degree of global symmetry whereas, melanomas exhibit multiple types of local symmetry embedded within their signature curves. We will then use ROC Analysis, a key statistical tool for evaluating detection, to characterize our diagnostic performance.

References

[1] Calabi, E., Olver, P., Shakiban, C., Tannenbaum, A., and Haker, S., *Differential and numerically invariant signature curves applied to object recognition*, Int. J. Computer Vision **26**, pp. 107-135(1998)).

[2] Boutin, M., *Numerically invariant signature curves*, Int. J. Computer Vision **40**, pp. 235-248 (2000).

[3] Hoff, D., and Olver, P.J.,*Extensions of invariant signatures for object recognition*, J. Math. Imaging Vision **45**, pp. 176-185 (2013).

[4] Grim, A., and Shakiban, C., *Applications of signatures in diagnosing breast tumors*, submitted for publication.

Walks in the quarter plane with multiple steps

M. Kauers[1], R. Yatchak[1]

[1] *Institute for Algebra, Johannes Kepler University, Linz, {manuel.kauers, rika.yatchak}@algebra.jku.at*

We extend the classification of nearest neighbour walks in the quarter plane to models in which multiplicities are attached to each direction in the step set. Our study leads to a small number of infinite families that completely characterize all the models whose associated group has order 4, 6, or 8. All these models have D-finite generating functions. We also discovered some new models with a group of order 10, whose generating function seems to be algebraic. According to our investigations, it remains true (and mysterious) that a model has a D-finite generating function if and only if its associated group is finite. This work has been accepted for publication at this year's conference on Formal Power Series and Algebraic Combinatorics (FPSAC). See [1] for a preprint.

References

[1] M. Kauers and R. Yatchak, *Walks in the Quarter Plane with Multiple Steps*, ArXiv 1411.3537, November 2014.

Computing Resolutions for Linear Differential Systems

Werner M. Seiler[1]

[1] *Institut für Mathematik, Universität Kassel, Germany, seiler@mathematik.uni-kassel.de*

Rings of linear differential operators represent a typical example of *polynomial algebras of solvable type*. This class of rings was first introduced by Kandry-Rody and Weispfenning [4] and various variants of it appear for instance in the work of Bueso et al. [3], Kredel [5], Levandovskyy [6] or the author [8]. It contains weakly non-commutative rings whose elements may be considered as polynomials in variables which do not necessarily commute and which may operate on the coefficients. From a theoretical point of view, these rings may have very different algebraic properties. However, from an algorithmic point of view, to all these rings the classical theory of Gröbner bases can be applied without changes, as one can meaningful work with leading terms and monomials.

In this talk we are mainly concerned with the problem of computing free resolutions over polynomial algebras of solvable type with special emphasis on the case of linear differential operators. In order to motivate this topic, we will first recall the relation between free resolutions over the ring of linear differential operators and compatibility complexes as they appear in the theory of overdetermined systems (see e. g. [10]). The former ones can be algorithmically computed – as discussed below – whereas the latter ones depend on the function space on which the operators act and may or may not exist. In the case that the function space is an injective cogenerator the two notions are dual to each other and each resolution yields immediately an exact compatibility complex (this observation follows essentially from results of Oberst [7]).

The main part of the talk will consists of a discussion under which conditions the theoretical results of [9] and the algorithmic results of [1] and [2] for the commutative polynomial ring remain valid for a polynomial algebra of solvable type.

In [8], the author presented an involutive version of the well-known Schreyer Theorem for Janet and Pommaret bases: given a Janet or Pommaret basis of a polynomial module, it shows how to read off a Janet or Pommaret basis of the first syzygy module from the involutive standard representations of the non-multiplicative prolongations of the generators. In contrast to the classical form of the Schreyer Theorem (which underlies most algorithms for computing resolutions), the involutive version allows to predict without any further computations the shape of the complete resolution obtained by iterating the theorem. In the case of a Pommaret basis, this resolution has even the same "bounding box" as the minimal one, i. e. we can read off the projective dimension and the Castelnuovo-Mumford regularity. As a trivial corollary, one then obtains Hilbert's Syzgy Theorem, i. e. the global dimension of the commutative polynomial ring.

In [1], the approach of [9] is complemented by Algebraic Discrete Morse Theory [11] in order to determine not only the shape but also the differential of the arising resolution. More precisely, it is shown how the results of [12] can be made effective via Pommaret bases (in [2], this is extended to Janet bases). This combination leads to a novel algorithm for the determination of free resolutions with very different features than previous algorithms. In particular, in the case that the notion of a minimal resolution is defined and thus one can speak of Betti numbers, this approach allows for the determination of individual Betti numbers without computing the minimal resolution. As benchmarks with a first prototypical implementation showed, the new algorithm is for many examples by orders of magnitude faster than previous ones.

References

[1] M. Albert, M. Fetzer, E. Sáenz-de-Cabezón and W.M. Seiler, *On the Free Resolution Induced by a Pommaret Basis*, J. Symb. Comp. **68**, pp. 4–26 (2015)

[2] M. Albert, M. Fetzer and W.M. Seiler, *Janet Bases and Resolutions in CoCoALib*, Preprint Universität Kassel (2015)

[3] J.L. Bueso, J. Gómez-Torrecillas and A. Verschoren, *Algorithmic Methods in Non-Commutative Algebra*, Mathematical Modelling: Theory and Applications 17, Kluwer, Dordrecht (2003)

[4] A. Kandry-Rody and V. Weispfenning, *Non-commutative Gröbner Bases in Algebras of Solvable Type*, J. Symb. Comp. **9**, pp. 1–26 (1990)

[5] H. Kredel, *Solvable Polynomial Rings*, Verlag Shaker (1993)

[6] V. Levandovskyy, *Non-commutative Computer Algebra for Polynomial Algebras: Gröbner Bases, Applications and Implementation*, Ph.D. thesis, Kaiserslautern (2005)

[7] U. Oberst, *Multidimensional Constant Linear Systems*, Acta Appl. Math. **20**, pp. 1–175 (1990)

[8] W.M. Seiler, *A Combinatorial Approach to Involution and δ-Regularity I: Involutive Bases in Polynomial Algebras of Solvable Type*, Appl. Alg. Eng. Comm. Comp. **20**, pp. 207–259 (2009)

[9] W.M. Seiler, *A Combinatorial Approach to Involution and δ-Regularity II: Structure Analysis of Polynomial Modules with Pommaret Bases*, Appl. Alg. Eng. Comm. Comp. **20**, pp. 261–338 (2009)

[10] W.M. Seiler, *Involution—The Formal Theory of Differential Equations and Its Applications in Computer Algebra*, Algorithms and Computations in Mathematics 24, Springer-Verlag, Heidelberg (2010)

[11] Sköldberg, E.: *Morse theory from an algebraic viewpoint*. Trans. Amer. Math. Soc. 358, 115–129 (2006)

[12] Sköldberg, E.: *Resolutions of modules with initially linear syzygies*. Preprint arXiv:1106.1913 (2011)

Computing Formal Solutions of Completely Integrable Pfaffian Systems With Normal Crossings

Maximilian Jaroschek[*]

May 12, 2015

Abstract

In this talk we are interested in the computation of formal solutions of completely integrable Pfaffian systems with normal crossings via rank reduction. Our investigations treat the generalization of known methods for the case of one or two variables to the multivariate setting. We follow the approach of the latter by associating to a given Pfaffian system a set of ordinary linear differential systems from which information on formal invariants can be retrieved. Furthermore, we introduce a variant of rank reduction facilitated by standard bases of modules over power series rings.

This is joint work with Moulay A. Barkatou and Suzy S. Maddah (University of Limoges, XLIM).

[*] Max Planck Institute for Informatics, Campus E1.4, 66123 Saarbrücken, Germany, `mjarosch@mpi-inf.mpg.de`

Conservation Laws and the Chazy Equation

T. M. N. Gonçalves [1], I. L. Freire [2]

[1] *Universidade Federal de Goiás, Catalao, Brazil, tmng@kentforlife.net*
[2] *Universidade Federal do ABC, Sao Paulo, Brazil, igor.freire@ufabc.edu.br*

Noether's theorem yields conservation laws for systems derived from a variational principle. As not all systems can be derived from a variational principle, the applicability of Noether's theorem is substantially reduced. Ibragimov in [1, 2] provided a solution to this problem through the construction of a Lagrangian for a system which is composed of the equation of interest and its adjoint equation.

Using these developments by Ibragimov and the new format for Noether's conservation laws (see [3, 4]) which is

$$\mathrm{d}\left(\mathscr{A}d(\rho)^{-1}\,(\upsilon_1,\dots,\upsilon_p)\,\mathsf{M}_{\mathscr{I}}\mathrm{d}\mathbf{x}\right)=0,$$

where $\mathscr{A}d(\rho)^{-1}$ is a moving frame, υ_i are vectors of invariants and $\mathsf{M}_{\mathscr{I}}$ comes from the action of the variational symmetry group on the volume form, can lead to the simplification of integration problems. In particular, here we will show how such conservation laws can be used to solve the Chazy equation,

$$y_{xxx}-2yy_{xx}+3y_x^2=0.$$

References

[1] N. H. Ibragimov, *Integrating factors, adjoint equations and Lagrangians*, J. Math. Anal. Appl. **318**, pp. 742–757 (2005).

[2] N. H. Ibragimov, *A new conservation theorem*, J. Math. Anal. Appl. **333**, pp. 311–328 (2006).

[3] T. M. N. Gonçalves and E. L. Mansfield, *On moving frames and Noether's conservation laws*, Stud. Appl. Math. **128**, pp. 1–29 (2011).

[4] T. M. N. Gonçalves and E. L. Mansfield, *Moving frames and Noether's conservation laws – the general case*, submitted to Forum Math. Sigma (2015).

Generalized Green's Operators and the Method of Characteristics

A. Korporal[1], G. Regensburger[2]

[1] *RICAM, Austrian Academy of Sciences, Linz, Austria, anja.korporal@oeaw.ac.at*
[2] *RICAM, Austrian Academy of Sciences, Linz, Austria, georg.regensburger@oeaw.ac.at*

Symbolic methods for solving and manipulating linear ordinary boundary problems in the framework of integro-differential operators have been presented in several previous AADIOS sessions. In this talk, we apply the well-known method of characteristics to present a possible extension to PDEs by translating them to a family of parametrized ODEs. Although usually applied to first-order equations, the method of characteristics can be generalized to any hyperbolic PDE, and we will show in several examples how our algorithms for factoring boundary problems or for computing compatibility conditions and generalized Green's Operators of overdetermined boundary problems can be applied in this case.

Use of a Two-Dimensional Operational Calculus for Nonlocal Vibration Boundary Value Problems

I. Dimovski[1], M. Spiridonova[2]

[1] *Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, dimovski@math.bas.bg*
[2] *Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, mspirid@math.bas.bg*

Nonlocal boundary value problems for the wave and the beam equations in finite space domains are considered. For solving such problems extensions of the Fourier method and the Duhamel principle are used in the frames of a two-dimensional operational calculus. Explicit formulae of the solutions are derived. These formulae can be used for numerical computation and visualization of the solutions. Examples with use of the computer algebra system *Mathematica* are included.

Symbolic Computation for Rankin-Cohen Differential Algebras

Eleanor Farrington[1], Emma Previato[2]

[1] *Massachusetts Maritime Academy, Buzzards Bay, MA 02532 efarrington@maritime.edu*
[2] *Department of Mathematics and Statistics, Boston University, Boston, MA 02215 ep@bu.edu*

Rankin-Cohen algebras were defined by Zagier [Z], who reprised the role of differential operators in the theory of modular forms, central in the 19th century but "surprisingly little (...) in more modern investigations". In brief, for $f(\tau)$ and $g(\tau)$ two modular forms of weights k, l respectively, on some group $\Gamma \subset PSL(2,\mathbb{R})$, let D be the differential operator $\dfrac{1}{2\pi\imath}\dfrac{d}{d\tau}$, given the expansion of the modular forms in τ, where $\dfrac{1}{2\pi\imath}\dfrac{d}{d\tau} = q\dfrac{d}{dq}$, $q = e^{2\pi\imath\tau}$ as usual. The n-th Rankin-Cohen bracket (so named by Zagier, after R.A. Rankin who studied the derivations on modular forms and H. Cohen who gave examples) of f and g is the only bilinear differential operator of degree $2n$ that acts on the graded vector space of modular forms on Γ, and is defined as follows (denoting $D^r f$ by $f^{(r)}$ for a form f):

$$[f,g]_n(\tau) = \sum_{r+s=n} (-1)^r \binom{n-k+1}{s}\binom{n-l+1}{r} f^{(r)}(\tau)g^{(s)}(\tau).$$

Zagier pursues the study of the algebraic structure that this operation gives to the ring of modular forms viewed as a differential module, observing that it is "not clear how far we would have to go to get the first relation or how much further to ensure that all subsequent relations obtained would be consequences of ones already found". Instead of determining the relations, he proposes the abstract concept of a Rankin-Cohen differential algebra and gives a "partial structure theorem".

In this work, we propose to use Symbolic Computation to detect minimal sets of relations for the case study of $\Gamma(7)$, the modular group of the Klein curve, the only algebraic curve of genus three with the largest possible group of automorphisms, motivated by the first-named author's Ph.D. Thesis [Farr], which uses techniques that allow us to deal explicitly with certain modular forms.

We apply the theory of Gröbner bases (as in [EGÔP]) to control the weight of the relations, and then perform a search (implemented in *Maple* syntax) for complete, minimal sets ot relations weight-by-weight; in consequence, our results only reach a(ny) finite given weight, but these relations are of interest, given the large number of open problems that concern the Klein curve (more specifically stated below).

Then, in order to further exploit the power of computation, we propose to study Rankin-Cohen differential algebras over finite fields; indeed, when giving their abstract definition in [Z], "We will suppose the ground field K to be of characteristic 0 (in our examples it is usually $\mathbb{Q}$ or $\mathbb{C}$) although it is clear that the theory makes sense in any characterisitc or, for that matter, even if we work over $\mathbb{Z}$ rather than a field." Since our strategy is to reduce cusp forms modulo a prime p, we assume that p does not divide the level [CFW], therefore $p \neq 7$ throughout.

1 Wronskians

The problem of determining the set of Weierstrass points on curves of arithmetic interest, such as the Fermat curves $x^N + y^N + z^N = 0$ and the modular curves $X(N)$, remains unsolved for all but a few values of N.

Klein's curve has been studied by its many different aspects according to the properties that were best accessible through one or the other: as a covering of $\mathbb{P}^1$, [FK1, VII.3], it is a Riemann surface M given by the algebraic equation

$$w^7 = z(z-1)^2.$$

The function z is ramified (of ramification number 7) at the points 0, 1 and ∞, and we set: $P_0 = z^{-1}(0), \quad P_1 = z^{-1}(1), \quad Q = z^{-1}(\infty)$, and consider the following divisors: $(z) = \dfrac{P_0^7}{Q^7}$, $(dz) = \dfrac{P_0^6 P_1^6}{Q^8}$, $(w) = \dfrac{P_0 P_1^2}{Q^3}$. Per this calculation, the differentials

$$\frac{dz}{w^3}, \quad (z-1)\frac{dz}{w^5}, \quad (z-1)\frac{dz}{w^6}$$

have divisors $P_0^3 Q, \quad P_0 P_1^3, \quad P_1 Q^3$, hence give a basis for $\Omega^1(M)$. Using this basis we can find an embedding of M in $\mathbb{P}^2$ [FK1, III.10]. In fact, if we set $w = -XY^{-1}, \quad z - 1 = X^3 Y^{-2}$ we find that the projective equation for the algebraic curve M is the quartic: $X^3Y + Y^3Z + Z^3X = 0$.

We can immediately conclude from the divisors of the differentials that the points P_0, P_1 and Q are Weierstrass points of weight 1. We turn to the Wronskian of to finish the search for the Weierstrass points. We recall that, denoting $W(f_1, \dots, f_g)$ the Wronskian determinant for a basis $f_1(z), \dots, f_r(z)$ of the canonical linear system, $|K|$, with associated linear series $\mathscr{L}(K)$, over an algebraic curve X of genus $g \geq 2$, in a local coordinate z, the zeros of $W(f_1, \dots, f_g)(dz)^{g(g+1)/2}$ are the Weierstrass points for the curve X, the multiplicities of the zeros being their Weierstrass weights [M, VII.4]. Using the function z above as a local coordinate, since we already took into account the points over 0, 1 and ∞ where it ramifies, we compute $W(z) = 3!(z^3 - 8z^2 + 5z + 1)/(z^8(z-1)^5)$ The polynomial

$p(z) = z^3 - 8z^2 + 5z + 1$ has three distinct real roots, each of which corresponds to 7 distinct points on M. Thus M has 24 Weierstrass points, each of weight one.

We now consider a second method for finding the ordinary Weierstrass points, as in [R]. When $X(\Gamma)$ is the modular curve $\Gamma \diagdown \mathscr{H}^*$, for Γ a subgroup of finite index in $SL_2(\mathbb{Z})$ and $\mathscr{H}^*$ the upper half plane with the cusps of Γ adjoined, the set of weight-2 cusp forms for Γ, $S_2(\Gamma)$, is isomorphic to the set of holomorphic 1-forms for the Riemann surface. Thus to build a Wronskian for $\Gamma \diagdown \mathscr{H}^*$ we may use a basis $f_1, f_2, \ldots, f_g$ for $S_2(\Gamma)$, the Wronskian $W(f_1, f_2, \ldots, f_g)$ being a modular form of weight $g(g+1)$ for Γ.

The Klein curve X is isomorphic to the modular curve $X(7)$, with $\Gamma = \Gamma(7)$. Since $\Gamma(7)$ is normal in $SL_2(\mathbb{Z})$, this Wronskian is a modular form for $SL_2(\mathbb{Z})$ itself, with character $\det \rho$, for ρ the natural representation of $SL_2(\mathbb{Z})$ on the space of cusp forms of weight 2 for Γ. The choice of basis only affects the Wronskian by a nonzero complex multiple, while we are only concerned about its zeros; to eliminate the dependence on the choice of basis entirely we may require that the first nonzero coefficient in the Fourier expansion of the Wronskian at the cusp at ∞ be 1. Thus we can talk about the Wronskian for $\Gamma \diagdown \mathscr{H}^*$.

In general, if the ramification index of Γ in $SL_2(\mathbb{Z})$ is r at ∞, we can express the Fourier expansion of $W(z)$ at ∞ as

$$W(z) = \sum_{n \geq n_0} a_n e^{2\pi i n z/r}, \quad a_{n_0} = 1.$$

For the case of $X(7)$, $g = 3$, so $W(z)$ is a cusp form of weight 12 with character for $SL_2(\mathbb{Z})$. The character factors through $SL_2(\mathbb{Z})/\{\pm 1\}\Gamma(7)$, hence is trivial, thus $W(z)$ is a cusp form for $SL_2(\mathbb{Z})$ itself. The only possibility is that $W(z) = \Delta$. Since Δ is never zero on $\mathscr{H}$, we find that the Weierstrass points are the cusps.

The Wronskian for the pluricanonical series, $\mathscr{L}(nK)$, $n \geq 2$ (associated to $|nK|$) gives the higher-order Weierstrass points [FK1, III.5]. In the pluricanonical case, the Wronskian for a modular curve $X(\Gamma)$ is an automorphic form of weight $(2n-1)^2 g(g-1)/2$ [FK2, 3.1].

Using the model for $X(7)$ given by $w^7 = z(z-1)^2$, we have found bases for the pluricanonical series $\mathscr{L}(nK)$ for X. Indeed, we observed that for $2 \leq n \leq 5$, pairwise multiplication of the elements of our previously found basis for $\mathscr{L}(K)$ leads to exactly $\dim \mathscr{L}(nK) = (2n-1)(g-1) - 1$ independent differentials. For example for $n = 2$, pairwise multiplication of the basis elements of $\mathscr{L}(K)$ above led to

$$\{\frac{1}{w^6}, \frac{1}{wz(z-1)}, \frac{1}{zw^3}, \frac{1}{w^2 z(z-1)}, \frac{1}{w^4 z}, \frac{1}{w^5 z}\}.$$

To use these Wronskians in the Rankin-Cohen algebra, we must find their q-expansion: our strategy is to first identify them as automorphic forms constructed from theta constants [FK2, III.2]; then use classical identities to embed (as Klein did) the curve in $\mathbb{P}^2$ [FK2, III.8.4]; and lastly, use an algebraic map to convert $\mathbb{P}^2$-coordinates into the meromorphic functions w,z on the curve as the 7-sheeted cover; retracing our steps, we have written the pluricanonical Wronskians as classical automorphic forms, and can Fourier-expand them. As Zagier notes, a "canonical" Rankin-Cohen algebra can be generated by a form in degree four and a degree-2 differentiation; our Wronskians are of course of higher degree, but he also considers, for comparison, a homogeneous generator F of arbitrary degree, provided it is not a zero-divisor, so our case study is a legitimate example of his theory.

2 Finite Fields

Modular forms in positive characteristic (we are only considering reduction of coefficient modulo a prime p, not Katz' theory which has an algebro-geometric definition and may give rise to non-liftable forms, an unsettled issue) still present challenges, such as the structure of their Hecke algebra [BK]. The Hecke operator makes sense in characteristic p, but others do not exist in characteristic zero, particularly "multiplication by the Hasse invariant"; the "theta operator" ϑ is defined in characteristic zero, in fact it is precisely what we called D following [Z], where it "destroys modularity" [K], but in positive characteristic it raises the weight by $p+1$: this $\vartheta := q\dfrac{d}{dq}$ acts formally on the q expansion of the discriminant Δ and the Eisenstein series E_4, E_6, and these can be chosen as generators of the (graded) ring of modular forms. In the recent monograph [K], the author implements some such operations in computation, using both MAGMA and its open-source counterpart SAGE, primarily with the goal of computing Fourier coefficients.

We propose to use our case-study $\Gamma(7)$ and computation in characteristic $p \neq 7$ (over a finite field or its algebraic closure), not only to study the structure of Rankin-Cohen algebras, but also with the goal of computing "theta cycles": these are specific to positive characteristic, and arise as follows. The multiplication $f \mapsto Af$, where A is the Hasse invariant, in characteristic p raises the weight by $p-1$ and leaves the q-expansion unchanged: the smallest weight in which a form f appears is called its "filtration" $w(f)$. Since $w(\vartheta^p f) = w(\vartheta f)$, one can attach to any mod p modular form f a $(p-1)$-tuple of integers, $\big(w(\vartheta f), w(\vartheta^2 f), \ldots, w(\vartheta^{p-1} f)\big)$, and this is called its theta cycle. These were investigated by J. Tate and classified by N. Jochnowitz in her thesis: they have applications to estimates on the number of local components of Hecke algebras. We study the action of the Rankin-Cohen brackets on theta cycles: this might give us an extra handle on the relations of Rankin-Cohen algebras in characterisitc p.

3 Conclusions

Our underlying theme is that the use of differential operators in the theory of modular forms, especially as regards their dual nature as algebro-geometric or number-theoretic objects, should be revived in the spirit of the nineteeth century and made powerful by means of symbolic computation. We use cusp forms over the Klein curve, obtain a relationship between the algebraic and modular aspects, and computationally obtain explicit identities for the little-known Rankin-Cohen differential (graded) algebras; in positive characteristic, even over finite fields, our case-study potentially aids the quest for the structure of the Hecke algebra. Further motivation for using the Klein curve is a computational study of its differential-Galois aspects (when viewed as an algebraic cover) [SU], which can be related to the algebraic Wronskians, and which we plan to relate to its cusp forms, particularly in positive characteristic since the previous work was carried out over the complex numbers.

References

[BK] Bellaïche, J.; Khare, C. Level 1 Hecke algebras of modular forms modulo *p*. Compos. Math. 151 (2015), no. 3, 397-415.

[CFW] Conrey, J. B.; Farmer, D. W.; Wallace, P. J. Factoring Hecke polynomials modulo a prime. Pacific J. Math. 196 (2000), no. 1, 123-130.

[EGÔP] J.C. Eilbeck, J. Gibbons, Y. Ônishi and E. Previato, From equations of Jacobians or Kummer varieties to Coble hypersurfaces, Preprint 2015.

[FK1] H. Farkas and I. Kra, Riemann Surfaces, 71, Graduate Texts in Mathematics, Springer-Verlag, New York, 1980.

[FK2] H. Farkas and I. Kra, Theta Constants, Riemann Surfaces and the Modular Group, 37, Graduate Studies in Mathematics, American Mathematical Society, Providence, R.I. 2001.

[Farr] E.S.A. Farrington, Aspects of Klein's Quartic Curve, Thesis (Ph.D.) Boston University. 2010. 172 pp. ISBN: 978-1124-05913-6 ProQuest LLC2010.

[K] Kilford, L. J. P. Modular forms. A classical and computational introduction. Imperial College Press, London, 2008.

[M] R. Miranda, Algebraic Curves and Riemann Surfaces, 5, Graduate Studies in Mathematics, American Mathematical Society, Providence, R.I. 1997.

[R] D.E. Rohrlich, *Some remarks on Weierstrass points*, in: Number theory related to Fermat's last theorem (Cambridge, MA, 1981), 71-78, Progr. Math., **26**, Birkhäuser, Boston, MA, 1982.

[SU] M.F. Singer and F. Ulmer, *On a third order differential equation whose differential Galois group is the simple group of* 168 *elements*, in: Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), Lecture Notes in Comput. Sci., Springer, Berlin, 316–324, 673, 1993.

[Z] D. Zagier, *Modular forms and differential operators*, in: K. G. Ramanathan memorial issue. Proc. Indian Acad. Sci. Math. Sci. 104 (1994), no. 1, 57-75.

Formal Solutions of Singularly-Perturbed Linear Differential Systems

M. A. Barkatou, S. S. Maddah

University of Limoges, XLIM, 123, Av. Albert Thomas, 87060 Limoges, France,
suzy.maddah@etu.unilim.fr, moulay.barkatou@unilim.fr

Given the singularly-perturbed linear differential system

$$\varepsilon^h \frac{dY}{dx} = A(x,\varepsilon)Y = \sum_{k=0}^{\infty} A_k(x)\varepsilon^k Y,$$

where h is an integer and the $A_k(x)$'s are $n \times n$ matrices whose entries lie in the ring of formal power series in x with complex coefficients.

Such systems are traced back to the year 1817 [10, Historical Introduction] and are exhibited in a myriad of problems within diverse disciplines including astronomy, hydrodynamic stability, and quantum physics [1, 5, 8]. Their study encompasses a vast body of literature as well (see, e.g., [2, 6, 8, 10] and references therein). In the case of a regular perturbation, i.e. $h \leq 0$, this system can be reduced to a set of nonhomogeneous unperturbed linear differential systems which can be solved successively. However, singular perturbations cause major complications. The difficulties are exhibited by the division of the domain $|x| \leq x_0$ into a finite number of subdomains in each of which the solutions, which have yet to be constructed, behave quite differently [3, 4]. The interest of this article is to construct an asymptotic representation of solutions in any of the corresponding subdomains.

We present an algorithm to compute the asymptotic representations of solutions of singularly-perturbed linear differential systems, in a neighborhood of a turning point. Our algorithm is based on an analysis by a Newton polygon and is implemented in the computer algebra system Maple [7].

Keywords: *Singularly-perturbed linear differential systems, turning points, Newton polygon, rank reduction, formal solutions, Maple.*

References

[1] C. M. Bender and S. A. Orszag. *Advanced mathematical methods for scientists and engineers I: Asymptotic methods and perturbation theory*. Vol. 1. Springer, 1999.

[2] G. Chen. Solutions Formelles de Systemes d'Equations Differentielles Lineaires Ordinaires Homogenes. PhD Thesis. Université Joseph Fourier. Grenoble 1. 1990.

[3] M. Iwano, On the study of asymptotic solutions of a system of linear ordinary differential equations containing a paramter. In *Japan Journal of Mathematics*, Vol. 35, pp 1-30, 1965.

[4] M. Iwano and Y. Sibuya. Reduction of the Order of a Linear Ordinary Differential Equation Containing a Small Parameter. *Kodai Math. Sem. Rep.*, 15, pp 1 - 28, 1963.

[5] C. C. Lin, The theory of hydrodynamic stability. *Cambridge Univ. Press*. Cambridge, 1966.

[6] Y.O. Macutan. Formal Solutions of Scalar Singularly-Perturbed Linear Differential Equations. *In Proceedings of the International Symposum on Symbolic and Algebraic Computation*, pp113-120. ACM Press, USA 1999.

[7] Maple Package for Symbolic Resolution of Singularly- Perturbed Linear Systems of Differential Equations. Available at: *http : //www.unilim.f r/pages_perso/suzy.maddah/*.

[8] J.A.M. McHugh. An historical Survey of Ordinary Linear Differential Equations with a Large Parameter and Turning Points. *Archive for History of Exact Sciences*, 7(4): pp 277-324,1971.

[9] W. Wasow. Topics in the Theory of Linear Ordinary Differential Equations Having Singularities with respect to a Parameter. *Institut de Recherche Mathématique Avancée*. Université Louis Pasteur. Strasbourg. 1979.

[10] W. Wasow. Linear Turning Point Theory. *Springer-Verlag*. 1985.

Localizable and Weakly Left Localizable Rings

V. V. Bavula[1]

[1] *University of Sheffield, UK, v.bavula@sheffield.ac.uk.*

Two new classes of rings, the class of left localizable and weakly left localizable rings, are introduced. A ring R is called *weakly left localizable* if each non-nilpotent element of R is invertible in some left localization $S^{-1}R$ of the ring R. Explicit criteria are given for a ring to be a weakly left localizable ring provided the ring has only finitely many maximal left denominator sets (eg, this is the case if a ring has a left Artinian left quotient ring).

Generalized morphisms – turning homological algorithms into closed formulas

M. Barakat[1]

[1] *RWTH Aachen University, Aachen, mohamed.barakat@rwth-aachen.de*

Homological algebra has the reputation of being the theory of abstract notions and lengthy complex constructions. Generalized morphism is a new notion or rather “data structure” which turns many of these constructions into simple closed formulas, easily implementable on a computer. I will demonstrate two applications of constructive spectral sequences.

Computing Liouvillian solutions of linear difference equations

T. Combot[1]

[1] *University of Burgundy, France, thierry.combot@u-bourgogne.fr*

We present an algorithm to compute Liouvillian solutions of linear difference equations with polynomials coefficients, without the problem of combinatorial search of singularities. The problem of computing Liouvillian solutions comes down to compute first order right factors of a difference operator $L \in \mathbb{Q}[n, \tau]$ but in an extended algebra $\mathscr{A}[\tau]$ where $\mathscr{A}$ is a finite difference ring extension over $\mathbb{Q}[n]$, the interlaced polynomials. This representation allows in particular to compute Liouvillian solutions in the same way as d'Alembertian solutions, the Galois group being by the way always connected over $\mathscr{A}$. A notion of exponential part for such solutions can be defined, and the problem comes down to try all possible exponential parts. Our approach is based on van Hoeijn method for factorizing differential operators: some particular singular solutions are computed and a right factor of L is searched by guessing an annihilating operator. This process, although not sufficient to obtain a complete factorization, is enough to compute all first order right factors. A particular attention will be given to the coefficient field, which can grow in the factorization computation, and in the complexity with respect to the degree in n of L. Several examples which were not accessible by previous methods will be presented.

Symbolic Computation in Studying the Restricted Three-Body Problem with Variable Masses

Alexander N. Prokopenya

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

The restricted three-body problem is a well-known model of celestial mechanics (see, for example, [1]). Recall that in the simplest case it describes a motion of the point P_2 of negligible mass in the gravitational field of two massive points P_0 and P_1, moving in Keplerian orbits about their common center of mass. It is assumed that the masses of points P_0 and P_1 are given and their orbits are completely determined by the known solution of the two-body problem. This problem is not integrable, and so the perturbation theory is usually applied to the analysis of the point P_2 motion. As a general solution of the two-body problem is known, one can consider in the first approximation that the point P_2 moves around the point P_0, for example, as a satellite and its Keplerian orbit is disturbed by the gravity of point P_1. Such a model has been used successfully in the study of satellite motion in the system Earth–Moon or Sun–planet [2, 3]. It was shown that doubly averaged equations of motion determining the evolution of satellite orbit may become integrable. The corresponding general solution may be found in analytic form, and it enables investigation of main qualitative features of the orbit parameters (see, for example, [4]).

We consider here a generalized case of a satellite version of the restricted three-body problem when two points P_0 and P_1 form a binary system, losing the mass due to the corpuscular and photon radiation (see [5]). We assume that the points masses vary isotropically with different rates with the only restriction that their total mass reduces according to the joint Meshcherskii law

$$\frac{m_{00}+m_{10}}{m_0(t)+m_1(t)} = \sqrt{At^2+2Bt+1} \equiv v(t) \ , \tag{1}$$

where $m_{00} = m_0(0)$, $m_{10} = m_1(0)$ are initial values of the points P_0, P_1 masses, and parameters A, B are chosen in such a way that $v(t)$ is an increasing function for $t > 0$. In this case equations of the points P_0, P_1 relative motion are integrable and their general solution can be written in symbolic form (see [6]).

We assume further that the point P_2 moves around point P_0, being perturbed by the gravity of point P_1. Besides, a distance between points P_0 and P_1 is assumed to be much greater than distance between points P_0 and P_2 and the Hill approximation [7] may be applied. Then the evolutionary equations determining long-term behaviour of the point P_2 orbital parameters become integrable and their solutions may be found in the analytical form (see [8, 9]).

The purpose of this paper is to present the main stages in the investigation of the restricted three-body problem with variable masses which requires tedious symbolic computations. Derivation of the evolutionary equations and determination of a class of functions $m_0(t)$, $m_1(t)$, satisfying equation (1), for which the evolutionary equations are integrable and describe a quasi-elliptic motion of the point P_2, is described in detail. All relevant calculation and visualization of the results are carried out using the Wolfram Mathematica.

References

[1] V. Szebehely. *Theory of orbits. The restricted problem of three bodies*, Academic Press, New York, London (1967).

[2] M.L. Lidov. *The evolution of orbits of artificial satellites of planets under the action of gravitational perturbations of external bodies*, Planetary and Space Science **9**, 10, pp. 719-759 (1962)

[3] M.L. Lidov, M.A. Vashkov'yak. *On quasi-satellite orbits in a restricted elliptic three-body problem*, Astron. Lett. **20**, 5, pp. 676-690 (1994).

[4] M.A. Vashkov'yak. *Evolution of orbits of distant satellites of Uranus*, Astron. Lett. **25**, 7, pp. 476-481 (1999).

[5] A.A. Bekov, T.B. Omarov. *The theory of orbits in non-stationary stellar systems*, Astron. Astrophys. Trans. **22**, pp. 145-153 (2003).

[6] L.M. Berkovič. *Gylden–Meščerski problem*, Cel. Mech. **24**, pp. 407-429 (1981).

[7] G.W. Hill. *Researches in the lunar theory*. Am. J. Math. **1**, pp. 129-147 (1878).

[8] A.N. Prokopenya, M.Zh. Minglibayev, B.A. Beketauov. *On integrability of evolutionary equations in the restricted three-body problem with variable masses*, in *Computer Algebra in Scientific Computing / CASC'2014*, V.P Gerdt, W. Koepf, E.W. Mayr, E.V. Vorozhtsov (ed.), LNCS 8660, Springer-Verlag, Heidelberg, pp. 375-389 (2014).

[9] A.N. Prokopenya, M.Zh. Minglibayev, B.A. Beketauov. *Secular perturbations of quasi-elliptic orbits in the restricted three-body problem with variable masses*. Int. J. Non-Lin. Mech. **73**, pp. 58-63 (2015).

One symbolical method for solving differential equations with delayed argument

Natasha Malaschonok

Tambov State University

Consider an equation

$$x^{(n)}(t)+\sum_{j=1}^{n}\sum_{k=0}^{N}a_{jk}x^{(n-j)}(t-t_k)=f(t), \tag{1}$$

with initial conditions $x^{(n-j)}(0)=x_0^{(n-j}, j=1,\dots,n$. The function $f(t)$ in the right-hand part is in general composite. We may consider for it the same partition points t_k.

All functions of the argument t are supposed to satisfy the conditions for existing of their Laplace transform, and they equal zero for negative t. The points $t_k, t_{k-1}<t_k$, are rational and taken in the set of $t\in\mathbf{T}: 0\le t\le T$. Writing t_k as $t_k=\frac{\tau_k}{\sigma_k}$, denote $\sigma=LCM_k(\sigma_k)$, and $t_k=\frac{\tilde{\tau}_k}{\sigma}$.

Preparation for Laplace transform

The unknown function $x(t)$ and $f(t)$ satisfy the properties, put on above, so the equation (1) may be written using the Heaviside function $\eta(t)$ in the following way:

$$x^{(n)}(t)+\sum_{j=1}^{n}\sum_{k=0}^{N}a_{jk}\eta(t-t_k)x^{(n-j)}(t-t_k)=f(t), \tag{2}$$

$f(t)$ is also written by means of Heaviside function.

Laplace transform

It permits to write symbolically the Laplace image of the equation (2):

$$\left(p^n+\sum_{j=1}^{n}\sum_{k=0}^{N}a_{jk}e^{-pt_k}p^{n-j}\right)X(p)= \tag{3}$$

$$\sum_{j=1}^{n}p^{j-1}x_0^{(n-j)}+\sum_{j=1}^{n-1}\sum_{k=0}^{N}a_{jk}p^{j-1}x_0^{(n-j)}e^{-pt_k}+F(p), \tag{4}$$

where $X(p)$ and $F(p)$ are the Laplace images of $x(t)$ and $f(t)$, correspondingly, and $F(p)$ in general is also a sum of exponents with polynomial coefficients.

Solving the algebraic equation

Denote

$$Q(p)=\sum_{j=1}^{n}p^{j-1}x_0^{(n-j)}+\sum_{j=1}^{n-1}\sum_{k=0}^{N}a_{jk}p^{j-1}x_0^{(n-j)}e^{-pt_k}+F(p), \tag{5}$$

$$D(p)=p^n+\sum_{j=1}^{n}\sum_{k=0}^{N}a_{jk}e^{-pt_k}p^{n-j}, \tag{6}$$

then

$$X(p)=\frac{Q(p)}{D(p)}. \tag{7}$$

Expansion of the solution in a series

Denote $e^{-\frac{p}{\sigma}}=z$. Then

$$X(p)=\frac{\sum_{j=1}^{n}p^{j-1}x_0^{(n-j)}+\sum_{j=1}^{n-1}\sum_{k=0}^{N}a_{jk}p^{j-1}x_0^{(n-j)}z^{\tilde{\tau}_k}+F(p)}{p^n+\sum_{j=1}^{n}\sum_{k=0}^{N}a_{jk}z^{\tilde{\tau}_k}p^{n-j}}. \tag{8}$$

Formally we expand (5) in a Taylor serious by z at the point $z=0$. It corresponds to $p:\mathrm{Re}p=+\infty$. Substituting $e^{-\frac{p}{\sigma}}$ instead of z, we obtain the series for $X(p)$ by $e^{-\frac{np}{\sigma}}$, which converges in some neighbourhood of ∞:

$$\sum_{n}A_n e^{-\frac{np}{\sigma}}, \tag{9}$$

where A_n are proper fractions, and can be represented as sums of partial fractions.

Inverse Laplace transform

For the series (6) the Inverse Laplace transform may be written symbolically.

We restrict ourselves to the consideration of one equation, but the method works similarly with systems of equations of such type.

Symbolic summation and integration: algorithms, complexity, and applications

Session Organizers

Carsten Schneider
Research Institute for Symbolic Computation
Johannes Kepler University
Carsten.Schneider@risc.jku.at

Eugene Zima
Physics and Computer Science
Wilfrid Laurier University
ezima@wlu.ca

Overview

The purpose of this session is to present some recent developments in the area of symbolic summation and symbolic integration, and their applications in combinatorics, number theory, particle physics, etc. It is also to highlight current state of the art in both - complexity analysis of summation and integration algorithms, and improvements in the complexity of aforementioned algorithms. Reports on the research in symbolic solution of difference equations and related fields are also most welcome.

Explicit generating series for small-step walks in the quarter plane

A. Bostan[1], F. Chyzak[1], M. van Hoeij[2], M. Kauers[3], L. Pech[4]

[1] *INRIA, Palaiseau, France, {alin.bostan,frederic.chyzak}@inria.fr*
[2] *Florida State University, Tallahassee, USA, hoeij@mail.math.fsu.edu*
[3] *RISC, Hagenberg, Austria, mkauers@gmail.com*
[4] *Google, Zürich, Switzerland, lucien.pech@gmail.com*

Lattice walks are combinatorial objects that occur frequently in discrete mathematics, statistical physics, probability theory, or operational research. The generating series that enumerate them under certain constraints interest both combinatorialists and the algorithmists of computer algebra. First, their algebraic properties vary greatly according to the family of admissible steps chosen to define them, making their generating series sometimes rational, sometimes algebraic (and therefore described by a polynomial equation), sometimes D-finite (and therefore described by a linear differential equation), or sometimes with no apparent equation. Since a few years, this has motivated an effort of classification that has resulted in characterizations that are not sufficiently understood yet to be fully explicit. In addition, the computational properties of lattice walks make them an interesting challenge for computer algebra: indeed, their description often leads to equations, whether polynomial or differential, whose degrees, orders, and sizes are so large that it becomes difficult to obtain those descriptions explicitly, and to manipulate them with reasonable efficiency.

Given a family of non-zero vectors of the plane with coordinates ± 1, vectors which we shall call "steps", a small-step walk on the plane, square lattice is a finite succession of steps located one after the other. We are particularly interested in walks that are constrained by being confined to the quarter plane (that is, with non-negative integer coordinates), and counted according to their length (number of steps). In this talk, we shall present a work in progress that makes a bridge between previous works of different natures on the topic of small-step walks on the quarter plane. On the one hand, Bousquet-Mélou and Mishna showed [2] that among the 79 essentially different models of walks, only 19 possess a D-finite and transcendental generating series, and thus correspond to linear differential equations, but without making explicit the differential equations whose existence they were proving. Almost simultaneously, Bostan et Kauers [1] performed non-trivial but heuristic computations to obtain linear differential equations most probably satisfied by the 19 walk models, but without formally proving the correctness of these equations. In the work described, we shall give the first proof that these equations are satisfied by the corresponding generating series. Our approach proceeds by representing the generating series of constrained walks as coefficient extractions in rational series, and by a thorough validation of the use of the creative-telescoping process [3] employed for these extractions.

Once proved, the differential equations allow to compute in a guaranteed way many formulas and properties of the walk series. First, a suitable factorization of the underlying linear differential operators combined with the algorithm of [4] allows to represent the walks geenerating series as variations of iterated primitives of Gauss hypergeometric series. It follows that algebraicity and transcendence properties of enumerative series and specializations that are significant to combinatorics are accessible to computation, as well as asymptotic formulas for a number of walk models counted by lengths.

References

[1] Alin Bostan and Manuel Kauers. Automatic classification of restricted lattice walks. In *21st International Conference on Formal Power Series and Algebraic Combinatorics (FPSAC 2009)*, Discrete Math. Theor. Comput. Sci. Proc., AK, pages 201–215.

[2] Mireille Bousquet-Mélou and Marni Mishna. Walks with small steps in the quarter plane. In *Algorithmic probability and combinatorics*, volume 520 of *Contemp. Math.*, pages 1–39. Amer. Math. Soc., Providence, RI, 2010.

[3] Frédéric Chyzak. An extension of Zeilberger's fast algorithm to general holonomic functions. *Discrete Math.*, 217(1-3):115–134, 2000.

[4] Tingting Fang and Mark van Hoeij. 2-descent for second order linear differential equations. In *ISSAC 2011—Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation*, pages 107–114. ACM, New York, 2011.

Definite Integration of Rational Functions

J. Gerhard[1]

[1] *Maplesoft, Waterloo ON, Canada,* `jgerhard@maplesoft.com`

Indefinite integration of rational functions has been a well-studied topic. Most computer algebra systems follow the text book algorithms, which first split the input rational function into a sum of polynomial part, rational part and transcendental part, and then integrate each of the three parts individually.

We will focus on the definite integration of the transcendental part, which is of the form g/f, where f and g are polynomials with coefficients in a field F of characteristic zero, f is monic, squarefree and non-constant, and g is nonzero and of lower degree than f. In particular, the talk will discuss how to evaluate limits of the antiderivative at $\pm\infty$ or at one of its discontinuities in closed form without the need to express the indefinite integral in terms of radicals.

The classical, straightforward formula for the indefinite integral of such a rational function is

$$\int \frac{g}{f}dx = \sum_{f(\alpha)=0} \frac{g(\alpha)}{f'(\alpha)} \ln(x-\alpha), \tag{1}$$

where the sum is over all roots α of f (which, by virtue of its squarefreeness, has only simple roots) and $g(\alpha)/f'(\alpha)$ is the residue of g/f at $x=\alpha$.

In the context of definite integration, say, over a real range $a..b$, a application of the Fundamental Theorem of Calculus (FTOC) to the antiderivative obtained from the classical formula may not be as straightforward as it sounds, due to branch cut issues. We illustrate this with a simple example.

$$F = \int \frac{dx}{x^2+1} = \sum_{\alpha^2=-1} \frac{\ln(x-\alpha)}{2\alpha} = \frac{i}{2}(\ln(x+i) - \ln(x-i)) \tag{2}$$

Note that, despite its appearance, F is actually real-valued. We apply FTOC to compute the improper integral from $-\infty..0$:

$$\int_{-\infty}^{0} \frac{dx}{x^2+1} = F(0) - \lim_{x\to\infty} F(-x) = -\frac{\pi}{2} - \frac{i}{2}\lim_{x\to\infty}(\ln(-x+i) - \ln(-x-i)) \tag{3}$$

The difficulty lies in evaluating the limit on the right. Each of the two logarithms is unbounded for $x\to\infty$, but the limit of the difference is finite. To see that, we rewrite each of the limits as follows:

$$\begin{aligned} \ln(i-x) &= \ln(x\cdot(-1+i/x)) = \ln(x) + \ln(-1+i/x), \\ \ln(-i-x) &= \ln(x\cdot(-1-i/x)) = \ln(x) + \ln(-1-i/x). \end{aligned}$$

The two $\ln(x)$ terms cancel, and for $x \to \infty$, we obtain

$$\begin{aligned}\lim_{x\to\infty}(\ln(-x+i)-\ln(-x-i)) &= \lim_{x\to\infty}\ln(-1+i/x)-\lim_{x\to\infty}\ln(-1-i/x)\\ &= \pi i-(-\pi i)=2\pi i\end{aligned}$$

Thus the definite integral (3) is evaluated as $\pi/2$, as expected.

In this derivation, we have used an explicit representation of the indefinite integral (2) in terms of radicals. However, it is well known from Galois theory that a representation in terms of radicals is not possible in general when the denominator polynomial is of degree 5 or higher, and even when it is, the corresponding radical expressions for the roots of f may become fairly unwieldy. Therefore it would be better if the limit could be computed using the implicit form (1).

Suppose again that our lower integration bound is $-\infty$, so we need to evaluate

$$\lim_{x\to\infty}\sum_{f(\alpha)=0}\frac{g(\alpha)}{f'(\alpha)}\ln(-x-\alpha). \tag{4}$$

Splitting the logarithm as $\ln(-x-\alpha)=\ln(x)+\ln(-1-\alpha/x)$ is valid in general when $x\to\infty$, but the limit for the second logarithm depends on the imaginary part of each particular root α:

$$\lim_{x\to\infty}\ln(-1-\alpha/x)=\begin{cases}\pi i & \text{if } \Im\alpha<0,\\ -\pi i & \text{if } \Im\alpha\geq 0\end{cases}$$

If f has only real roots, then the limit is $-\pi i$ for each such root, and we can find a closed form for the limit:

$$\begin{aligned}\lim_{x\to\infty}\sum_{f(\alpha)=0}\frac{g(\alpha)}{f'(\alpha)}\ln(-x-\alpha) &= (\ln(x)-\pi i)\lim_{x\to\infty}\sum_{f(\alpha)=0}\frac{g(\alpha)}{f'(\alpha)}\\ &= \begin{cases}0 & \text{if } \deg g\leq \deg f-2,\\ -\infty-\pi i & \text{if } \deg g=\deg f-1 \text{ and } \mathrm{lc}(g)>0,\\ \infty+\pi i & \text{if } \deg g=\deg f-1 \text{ and } \mathrm{lc}(g)<0,\end{cases}\end{aligned}$$

where $\mathrm{lc}(g)$ is the leading coefficient of g. In the general case, when f has non-real roots, it is not clear how to find a closed form for the limit without using radicals.

Besides the classical formula (1), other approaches to finding antiderivatives of rational functions with squarefree denominators have been proposed and widely implemented, with the goal of minimizing the size of the algebraic extension required to express the indefinite integral in closed form [2, 3, 4, 1]. These lead to antiderivatives of the form

$$\int\frac{g}{f}dx=\sum_{r(\beta)=0}\beta\ln s(\beta,x), \tag{5}$$

where r is a nonconstant univariate polynomial and s is a bivariate polynomial in β and x. Every root β of r is a residue $g(\alpha)/f'(\alpha)$, and the main advantage of these methods is that the minimal polynomial of β, which is r or a divisor of r, has smaller degree than f.

In this formulation, even though the degree of the algebraic extension is possibly lower, it is even less obvious how to find closed forms for the limit of the antiderivative, since in general s, the argument of the logarithm, is of degree 2 or higher.

Additional difficulties arise when the interval of integration contains poles of the integrand. In such a situation, the definite integral is undefined, but it can still be given a finite value as a Cauchy principal value integral. Then, in addition to the limits of the antiderivative at the integration bounds, limits at the poles of the integrand have to be computed.

The talk discusses new ways of evaluating such limits in closed form, by directly using one of the implicit representations (1) or (5), without the need to use radicals. Special cases such as when all roots of f are real, or when all roots are on the imaginary axis, can be recognized and lead to simpler formulas. In the general case, implicit representations for specific roots of f, such as, e.g., isolating intervals for real roots, are used.

References

[1] D. Lazard and R. Rioboo, *Integration of Rational Functions: Rational Computation of the Logarithmic Part*, Journal of Symbolic Computation **9**, pp. 123-151 (1997).

[2] M. Rothstein, *Aspects of symbolic integration and simplification of exponential and primitive functions*, Phd thesis, University of Wisconsin-Madison (1976).

[3] M. Rothstein, *A new algorithm for the integration of exponential and logarithmic functions*, in *Proceedings of the 1977 MACSYMA Users Conference, Berkeley CA*, NASA, Washington DC, pp. 263-274 (1977).

[4] B. M. Trager, *Algebraic Factoring and Rational Function Integration*, in *Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation SYMSAC '76, Yorktown Heights NY*, ed. R. D. Jenks, ACM Press, pp. 219-226 (1976).

Creative Telescoping via Hermite Reduction

S. Chen[1], H. Huang[1,2], M. Kauers[2], Z. Li[2].

[1] *Institute for Systems Sciences, Chinese Academy of Sciences, Beijing, China,*
[2] *Institute for Algebra, Johannes Kepler University, Linz, Austria, {hui.huang, manuel.kauers}@algebra.jku.at*

Creative telescoping is a key tool in symbolic summation and integration. It is used for constructing for a given definite sum or integral an associated linear recurrence or differential equation, which can then be used by other algorithms for finding out all sorts of interesting facts about the quantity in question. Four generations of creative telescoping algorithms can be distinguished: the first was based on elimination in ideals of operator algebras. The second is the classical Zeilberger algorithm and its variants. The third goes back to an idea of Apagodu and Zeilberger. These algorithms are particularly easy to implement and to analyze, but may not find optimal solutions. The fourth and final (so far) generation of creative telescoping algorithms is based on Hermite reduction. This idea was first worked out for definite integrals of multivariate rational functions by Chen in his PhD thesis. It has since been extended to more general classes of sums and integrals. In the talk, we will explain the idea of this apprach and a striking advantage over earlier algorithms. We will also present a Hermite-reduction based algorithm applicable to definite hypergeometric sums, published this year at ISSAC [1].

References

[1] S. Chen, H. Huang, M. Kauers and Z. Li, *A Modified Abramov-Petkovsek Reduction and Creative Telescoping for Hypergeometric Terms*, Proceedings of ISSAC'15, to appear.

Harmonic sums and polylogarithms at negative multiple-indices

Gérard H. E. Duchamp$^\heartsuit$ - Hoang Ngoc Minh$^\diamondsuit$ - Ngo Quoc Hoan$^\clubsuit$

$^\heartsuit$ *Paris XIII University, 93430 Villetaneuse, France, gheduchamp@gmail.com*
$^\diamondsuit$ *Lille II University, 59024 Lille, France, hoang@univ-lille2.fr*
$^\clubsuit$ *Paris XIII University, 93430 Villetaneuse, France, quochoan_ ngo@yahoo.com.vn*

Abstract

Extending the Faulhaber's formula, the Bernoulli polynomials and the Eulerian polynomials, we study the multi-indexed harmonic sums and polylogarithms. Our techniques are based on the combinatorics of the noncommutative generating series in the quasi-shuffle[1] Hopf algebra.

1 Introduction

In this paper, in order to implement the renormalization of the following divergent polyzetas [11, 12, 6]

$$\sum_{n_1>\ldots>n_r>0} n_1^{s_1}\ldots n_r^{s_r},\quad\text{for}\quad s_1,\ldots,s_r\in\mathbb{N},$$

we study, via the combinatorics of noncommutative generating series in the Hopf quasi-shuffle algebra [9, 10], the relations among *harmonic sums* and *polylogarithms*, indexed by the words $y_{s_1}\ldots y_{s_r}$ belonging to the monoid Y_0^*, generated by the alphabet $Y_0=\{y_k\}_{k\geq 0}$ and among their noncommutative generating series. They are defined as follows

$$\mathrm{H}^-_{y_{s_1}\ldots y_{s_r}}(N):=\sum_{n_1>\ldots>n_r>0}^{N} n_1^{s_1}\ldots n_r^{s_r}\quad\text{and}\quad \mathrm{Li}^-_{y_{s_1}\ldots y_{s_r}}(z):=\sum_{n_1>\ldots>n_r>0} n_1^{s_1}\ldots n_r^{s_r}z^{n_1},$$

where $r,N\in\mathbb{N}_+$ and $z\in\mathbb{C}$ such that $\mid z\mid<1$. In particular, for $r\in\mathbb{N}_+$, we have

$$\mathrm{H}^-_{y_0^r}(N)=\binom{N}{r}\quad\text{and}\quad \mathrm{Li}^-_{y_0^r}(z)=\left(\frac{z}{1-z}\right)^r.$$

Let us introduce also the following noncommutative generating series[2], for $t\in\mathbb{C}$,

$$\mathrm{H}^-(N):=\sum_{w\in Y_0^*}\mathrm{H}^-_w(N)\,w\quad\text{and}\quad\Theta(t):=\sum_{w\in Y_0^*}t^{(w)+|w|}w=\Big(\sum_{y\in Y_0}t^{(y)+1}y\Big)^*,\tag{1}$$

$$\mathrm{L}^-(z):=\sum_{w\in Y_0^*}\mathrm{Li}^-_w(z)\,w\quad\text{and}\quad\Lambda(t):=\sum_{w\in Y_0^*}((w)+\mid w\mid)!t^{(w)+|w|}w,\tag{2}$$

$$C^-:=1_{Y_0^*}+\sum_{w\in Y_0Y_0^*}C^-_w\,w,\quad\text{where}\quad C^-_w:=\prod_{w=uv,v\neq 1_{Y_0^*}}\frac{1}{(v)+\mid v\mid}.\tag{3}$$

[1] The quasi-shuffle product is denoted by $⧢$ and its coproduct by $\Delta_{⧢}$.

[2] We denote the length and the weight of $w=y_{s_1}\ldots y_{s_r}\in Y_0^*$ by the numbers $\mid w\mid=r$ and $(w)=s_1+\ldots+s_r$, respectively.

2 Main results

For harmonic sums, we define, firstly, the *multiple Bernoulli polynomials* $\{B_{y_{n_1}\dots y_{n_r}}\}_{n_1,\dots,n_r\in\mathbb{N}}$ by their commutative exponential generating series as follows

$$\sum_{n_1,\dots,n_r\in\mathbb{N}} B_{y_{n_1}\dots y_{n_r}}(z)\frac{t_1^{n_1}\dots t_r^{n_r}}{n_1!\dots n_r!} = \frac{t_1\dots t_r e^{z(t_1+\dots+t_r)}}{\prod\limits_{k=1}^{r}(e^{t_k+\dots+t_r}-1)}, \quad \text{for} \quad z\in\mathbb{C},$$

or by the following difference equation, for $n_1\in\mathbb{N}_+$,

$$B_{y_{n_1}\dots y_{n_r}}(z+1) = B_{y_{n_1}\dots y_{n_r}}(z) + n_1 z^{n_1-1} B_{y_{n_2}\dots y_{n_r}}(z).$$

For any $w\in y_s Y_0^*, s>1$, we have $B_w(1)=B_w(0)$. Then let us define also[3] $b_w := B_w(0)$ and $\beta_w(z) := B_w(z) - b_w$. In the same way, for polylogarithms, we extend the Eulerian polynomials [5] as follows, for any $w\in Y_0^*$,

$$A_w^-(z) := \begin{cases} 1 & \text{if} \quad w = y_0, \\ \sum\limits_{k=0}^{s_1-1} A_{s_1,k} z^k & \text{if} \quad w = y_{s_1}\in Y_0 - \{y_0\}, \\ \sum\limits_{i=0}^{s_1}\binom{s_1}{i} A_{y_i}^-(z) A_{y_{s_1+s_2-i}y_{s_3}\dots y_{s_r}}^-(z) & \text{if} \quad w = y_{s_1}\dots y_{s_r}\in Y_0Y_0^*, z\in\mathbb{C}, \end{cases}$$

where $A_{s_1,k}$ are Eulerian numbers. We obtain then the following results

1. For any $w\in Y_0^*, N\in\mathbb{N}_+$ and $z\in\mathbb{C}$ such that $\mid z\mid< 1$, $\mathrm{Li}_w^-(z)$ and $\mathrm{H}_w^-(N)$ are polynomials, with rational coefficients on $(1-z)^{-1}$ and N respectively, of valuation 1 and of degree $(w)+|w|$. Moreover,

$$\lim_{N\to+\infty}\frac{\mathrm{H}_w^-(N)}{N^{(w)+|w|}} = \lim_{z\to1}\frac{(1-z)^{(w)+|w|}}{((w)+\mid w\mid)!}\mathrm{Li}_w^-(z) = C_w^-\in\mathbb{Q}.$$

2. For any $n_1,\dots,n_r,N\in\mathbb{N}_+$, we have[4]

$$\beta_{y_{n_1}\dots y_{n_r}}(N) = \sum_{k=1}^{r}(\prod_{i=1}^{k} n_i) b_{y_{n_{k+1}}\dots y_{n_r}} \mathrm{H}^-_{y_{n_1-1}\dots y_{n_k-1}}(N-1),$$

$$\mathrm{H}^-_{y_{n_1}\dots y_{n_r}}(N) = \frac{\beta_{y_{n_1+1}\dots y_{n_r+1}}(N+1) - \sum\limits_{k=1}^{r-1} b_{y_{n_{k+1}+1}\dots y_{n_r+1}}\beta_{y_{n_1+1}\dots y_{n_k+1}}(N+1)}{\prod\limits_{i=1}^{r}(n_i+1)}. \quad (4)$$

[3] The number b_w is also called *multiple Bernoulli number* which differ from those defined in [3, 8] or in [11, 12].

[4] The identity (4) extends the Johann Faulhaber's formula (obtained for $r=1$) [4].

3. For any $w = y_{s_1} \ldots y_{s_r} \in Y_0^*$, we get on the one hand[5]

$$\mathrm{Li}_w^-(z) = (\theta_0^{s_1+1}\iota_1)\ldots(\theta_0^{s_{r-1}+1}\iota_1)\,\mathrm{Li}_{y_{s_r}}^-(z) = \left(\frac{z}{1-z}\right)^{|w|}\frac{A_w^-(z)}{(1-z)^{(w)}},$$

and on the other hand

   (a) If $r = 1$, then we have $\mathrm{Li}_{y_{s_1}}^-(z) = \sum_{k=1}^{s_1} S_2(s_1,k)k!\frac{z^k}{(1-z)^{k+1}}$, where $\{S_2(s_1,k)\}_{1\le k\le s_1}$ are the Stirling numbers of second kind. Hence,

$$\forall k \in \mathbb{N}_+, \qquad \frac{1}{(1-z)^k} = \frac{(-1)^{k+1}}{1-z} + \sum_{j=2}^{k}\frac{(-1)^{k+j}S_1(k,j)}{k!}\,\mathrm{Li}_{y_{j-1}}^-(z),$$

   where $\{S_1(s_1,k)\}_{1\le k\le s_1}$ are the Stirling numbers of first kind.

   (b) If $r > 1$ then $\mathrm{Li}_{y_{s_1}\ldots y_{s_r}}^-(z) = \left(\frac{z}{1-z}\right)^{|w|}\sum_{i=r}^{s_1+\ldots+s_r}\sum_{j=0}^{s_1\ldots+s_{r-1}} l_{i,j}\frac{z^{i-1-j}}{(1-z)^i}$, where for $r \le i \le s_1+\ldots+s_r$ and $0 \le j \le s_1+\ldots+s_{r-1}$, $l_{i,j}$ are defined as follows,

$$l_{ij} = \sum_{\substack{1\le k_t\le s_t\\ k_1+\ldots+k_r=i}}\left(\prod_{n=1}^{r}(k_n!S_2(s_n,k_n))\right)\sum_{\substack{0\le t_m\le k_m;\forall m=1,\ldots,r-1\\ t_1+\ldots+t_{r-1}=j}}\prod_{p=1}^{r-1}$$
$$\binom{k_r+\ldots+k_{r-p+1}+p-t_{r-p+1}-\ldots-t_{r-1}}{t_{r-p}}\binom{k_{r-p}+t_{r-p+1}+\ldots t_{r-1}}{k_{r-p}-t_{r-p}}.$$

4. The noncommutative generating series H^- and C^- are group-like, for $\Delta_{\shuffle}$, and[6]

$$\lim_{N\to+\infty}\Theta^{\odot-1}(N)\odot\mathrm{H}^-(N) = \lim_{z\to1}\Lambda^{\odot-1}((1-z)^{-1})\odot\mathrm{L}^-(z) = C^-.$$

5. There is a law of algebra $\top$ which is not dualizable in $\mathbb{Q}\langle Y_0\rangle$ [7] such that the following maps are surjective morphisms of algebras

$$\mathrm{H}_\bullet^- : (\mathbb{Q}\langle Y_0\rangle, \shuffle) \longrightarrow (\mathbb{Q}\{\mathrm{H}_w^-\}_{w\in Y_0^*},.), \qquad w \longmapsto \mathrm{H}_w^-,$$
$$\mathrm{Li}_\bullet^- : (\mathbb{Q}\langle Y_0\rangle, \top) \longrightarrow (\mathbb{Q}\{\mathrm{Li}_w^-\}_{w\in Y_0^*},.), \qquad w \longmapsto \mathrm{Li}_w^-.$$

   Moreover, $\ker\mathrm{H}_\bullet^- = \ker\mathrm{Li}_\bullet^- = \mathbb{Q}\langle\{w - w\top 1_{Y_0^*} | w \in Y_0^*\}\rangle$.

6. Let $\top' : \mathbb{Q}\langle Y_0\rangle \times \mathbb{Q}\langle Y_0\rangle \longrightarrow \mathbb{Q}\langle Y_0\rangle$ be a law such that $\mathrm{Li}_\bullet^-$ is a morphism for $\top'$ and such that $(1_{Y_0^*}\top'\mathbb{Q}\langle Y_0\rangle)\cap\ker(\mathrm{Li}_\bullet^-) = \{0\}$. Then $\top' = g\circ\top$ where $g \in GL(\mathbb{Q}\langle Y_0\rangle)$ such that $\mathrm{Li}_\bullet^-\circ g = \mathrm{Li}_\bullet^-$.

7. $\{\mathrm{H}_{y_k}^-\}_{k\ge0}$ (resp. $\{\mathrm{Li}_{y_k}^-\}_{k\ge0}$) are $\mathbb{Q}-$ linearly independent.

[5] Here, we use the operators over polylogarithms $\theta_0 : g(z) \longmapsto z\frac{d}{dz}g(z)$ and $\iota_1 : g(z) \longmapsto \int_0^z \frac{g(t)dt}{1-t}$.

[6] Here, the Hadamard product is denoted by $\odot$ and its dual law is denoted by $\Delta_\odot$. The inverses of Θ and Λ, for the Hadamard product [13], are denoted respectively by $\Theta^{\odot-1}$ and $\Lambda^{\odot-1}$ (their coefficients do not vanish). One obtains then an Abel like theorem for the noncommutative generating series given in (1),(2) and (3).

References

[1] G.H.E. Duchamp, S.Goodenough and K.A. Penson– *Rational Hadamard products via Quantum Diagonal Operators*,
Arxiv arXiv:0810.3641 [cs.SC]

[2] Pawel Blasiak, Philippe Flajolet– *Combinatorial Models of Creation-Annihilation* Séminaire Lotharingien de Combinatoire, B65c (2011)

[3] T. Arakawa, M. Kaneko– *Multiple zeta values, poly-Bernoulli numbers, and related zeta functions*, Nagoya Math. J. 153 (1999), 189-209.

[4] J. Faulhaber– *Darinnen die miraculosische Inventiones zu den hochsten Cossen weiters continuirt und profitiert werden*, Academia Algebrae (1631).

[5] D. Foata, M.-P. Schützenberger– *Théorie Géométrique des Polynômes Eulériens*, Lecture Notes in Mathematics, Springer-Verlag, Berlin, Heidelberg, New York, (1970), 138.

[6] H. Furusho, Y. Komori, K. Matsumoto, H. Tsumura– *Desingularization of multiple zeta-functions of generalized Hurwitz-Lerch type*, 2014.

[7] V.C. Bui, G.H.E. Duchamp, N. Hoang, V. Hoang Ngoc Minh, C. Tollu– *Combinatorics on the ϕ-deformed stuffle product*, arXiv:1302.5391

[8] Hoang Ngoc Minh– *Finite polyzêtas, Poly-Bernoulli numbers, identities of polyzêtas and noncommutative rational power series*, in the proceeding of 4-th International Conference on Words, pp. 232-250, September, 10-13, 2003, Turku, Finland.

[9] Hoang Ngoc Minh– *On a conjecture by Pierre Cartier about a group of associators*, Acta Math. Vietnamica (2013), 38, Issue 3, pp. 339-398.

[10] Hoang Ngoc Minh– *Structure of polyzetas and Lyndon words*, Vietnamese Math. J. (2013), 41, Issue 4, pp. 409-450.

[11] Guo L., B. Zhang– *Renormalization of multiple zeta values*, Journal of Algebra 319 (2008): 3770-809.

[12] D. Manchon, S. Paycha– *Nested sums of symbols and renormalized multiple zeta values*, International Mathematics Research Notices, Vol 2010, N. 24, p. 4628-4697.

[13] C. Reutenauer– *Sur les éléments inversibles de l'algèbre de Hadamard des séries rationnelles*, Bulletin de la Société Mathématique de France, 110 (1982), p. 225-232

Symbolic integration of multiple polylogarithms

E. Panzer

CNRS and IHES, Bures-sur-Yvette, France, erikpanzer@ihes.fr

Multiple polylogarithms are (locally) analytic, transcendental functions of several complex variables which generalize the logarithm $\mathrm{Li}_1(z) = -\log(1-z)$ to

$$\mathrm{Li}_{n_1,\ldots,n_d}(z_1,\ldots,z_d) = \sum_{0<k_1<\cdots<k_d} \frac{z_1^{k_1}\cdots z_d^{k_d}}{k_1^{n_1}\cdots k_d^{n_d}} \quad \text{where} \quad n_1,\ldots,n_d \in \mathbb{N}. \tag{1}$$

They have many applications in mathematics but also in physics, where they occur frequently in computations of Feynman integrals. The algebra of rational linear combinations of such functions is in general not closed under integration, but there are special situations (subalgebras) where indeed the integral can itself be expressed in terms of multiple polylogarithms and their special values. For example,

$$\int_0^\infty \int_0^\infty \frac{\log(1+1/(xz))\,\mathrm{d}x\,\mathrm{d}y}{(1+y)(1+x+y+1/z)} = \zeta(3) - \frac{\pi^2}{6}\log(z) - \mathrm{Li}_{1,2}(1,-z) - \mathrm{Li}_3(-z) \tag{2}$$

with the Riemann zeta value $\zeta(3) = \sum_{k=1}^\infty k^{-3} = \mathrm{Li}_3(1)$. We sketch the algorithms from [1, 2] for symbolic computation of such integrals. These are based on representations in terms of *hyperlogarithms*, a family of iterated integrals of the form

$$L_{\sigma_1,\ldots,\sigma_n}(z) = \int_0^z \frac{\mathrm{d}z_1}{z_1-\sigma_1}\int_0^{z_1}\frac{\mathrm{d}z_2}{z_2-\sigma_2}\cdots\int_0^{z_{n-1}}\frac{\mathrm{d}z_n}{z_n-\sigma_n}. \tag{3}$$

The necessary condition of *linear reducibility* will be explained and we present our Maple implementation `HyperInt` [2], which has been applied successfully [3, 4] to compute many (including hitherto unknown) Feynman integrals. It may be useful in other applications as well, whenever integrals similar in spirit to Eq. (2) occur.

References

[1] F. C. S. Brown, *The Massless Higher-Loop Two-Point Function*, Commun. Math. Phys. **287**, pp. 925–958 (2009).

[2] E. Panzer, *Algorithms for the symbolic integration of hyperlogarithms with applications to Feynman integrals*, Comput. Phys. Commun. **188**, pp. 148–166 (2015).

[3] E. Panzer, *On hyperlogarithms and Feynman integrals with divergences and many scales*, JHEP **2014**, 71 (2014).

[4] E. Panzer, *On the analytic computation of massless propagators in dimensional regularization*, Nucl. Phys. B **874**, pp. 567–593 (2013).

Algorithms in symbolic integration

Clemens G. Raab[1]

[1] *RICAM, Austrian Academy of Sciences, Linz, Austria, clemens.raab@oeaw.ac.at*

The goal of this talk is to give a brief overview of some techniques and algorithms for symbolic computation of one-dimensional integrals. Both indefinite integration and computation of parameter integrals will be covered. Most notably we will discuss some variants of Risch's algorithm [2, 7, 5, 1]. Several other methods will be presented as well and many examples will be given.

References

[1] Stefan T. Boettner, *Mixed Transcendental and Algebraic Extensions for the Risch-Norman Algorithm*, PhD Thesis, Tulane University, New Orleans, USA (2010).

[2] Manuel Bronstein, *Symbolic Integration I — Transcendental Functions*, 2nd ed., Springer (2005).

[3] Shaoshi Chen, Manuel Kauers, Christoph Koutschan, *A Generalized Apagodu-Zeilberger Algorithm*, in *Proceedings of ISSAC 2014*, K. Nabeshima (ed.), pp. 107–114 (2014).

[4] Frédéric Chyzak, *An extension of Zeilberger's fast algorithm to general holonomic functions*, Discrete Mathematics **217**, pp. 115–134 (2000).

[5] Arthur C. Norman, P. M. A. Moore, *Implementing the new Risch Integration algorithm*, in *Proceedings of the 4th International Colloquium on Advanced Computing Methods in Theoretical Physics*, A. Visconti et al. (eds.), pp. 99–110 (1977).

[6] Jean C. Piquette, A. L. Van Buren, *Technique for evaluating indefinite integrals involving products of certain special functions*, SIAM J. Math. Anal. **15**, pp. 845–855 (1984).

[7] Clemens G. Raab, *Definite Integration in Differential Fields*, PhD Thesis, Johannes Kepler University, Linz, Austria (2012).

[8] Albert D. Rich, David J. Jeffrey, *A Knowledge Repository for Indefinite Integration Based on Transformation Rules*, in *Proceedings of Calculemus/MKM 2009*, J. Carette et al. (eds.), pp. 480–485, 2009.

[9] Robert H. Risch, *The problem of integration in finite terms*, Trans. Amer. Math. Soc. **139**, pp. 167–189 (1969).

Refined Holonomic Summation Meets Particle Physics

Johannes Blümlein,[1] Mark Round,[1, 2, *] and Carsten Schneider[2]

[1] *Deutsches Elektronen-Synchrotron, DESY, Platanenallee 6, 15738, Zeuthen, Germany.*
[2] *Research Institute for Symbolic Computation (RISC),*
Johannes Kepler University, Altenbergerstraße 69, A-4040, Linz, Austria.

Definite nested multi-sums and infinite multi-sums, both with hypergeometric summands, occur as a fundamental problem in calculating Feynman diagrams [1]. In this talk a short outline of this problem is given. A review of the main paradigm of creative telescoping is given with emphasis on techniques for multi-sums. Established techniques to handle these particle physics sums [2] do not fully exploit the available mathematical structures. A new method of handling definite nested multi-sums through refined holonomic summation is introduced for this reason. The technical details regarding possible scenarios and efficiency considerations are given. A recent example of a particle physics problem solved using an implementation of the refined holonomic approach is outlined to show the scope of the new method in physics problems.

REFERENCES

[1] J. Blumlein, S. Klein, C. Schneider, and F. Stan, (2010), arXiv:1011.2656 [cs.SC].
[2] C. Schneider, J.Phys.Conf.Ser. **523**, 012037 (2014), arXiv:1310.0160 [cs.SC].

[*] mark.round@desy.de

Refined Parameterized Telescoping Algorithms

C. Schneider[1]

[1] *Research Institute for Symbolic Computation (RISC), Johannes Kepler University, Linz, Austria, cschneid@risc.jku.at*

The summation paradigm of parameterized telescoping plays a prominent role in symbolic summation: it covers as special cases telescoping and creative telescoping, and enables one to find all algebraic relations among indefinite sums. In [1] Karr introduced ΠΣ-fields, a general class of difference fields, and solved this problem for indefinite nested sums and products covering as special cases, e.g., the (q–)hypergeometric summation and their mixed versions. In this talk we present enhanced algorithms for this problem by constructing refined difference fields [2]. In this way, one can find improved sum representations and can hunt for linear recurrences with smaller recurrence orders.

References

[1] M. Karr. Summation in finite terms. *J. ACM*, 28:305–350, 1981.

[2] C. Schneider. Fast algorithms for refined parameterized telescoping in difference fields. In: Computer Algebra and Polynomials, Applications of Algebra and Number Theory, Jaime Gutierrez, Josef Schicho, Martin Weimann (ed.), Lecture Notes in Computer Science (LNCS) 8942, pp. 157-191. 2015. Springer, ISSN: 0302-9743. arXiv:1307.7887 [cs.SC].

Dispersion and complexity of indefinite summation

E. Zima[1]

[1] *Wilfrid Laurier University, Waterloo, Canada, ezima@wlu.ca*

The notion of *dispersion* plays a crucial role in the development of modern algorithms for indefinite summation. First introduced by Abramov in his classical work [1] as the maximal integer distance between roots of the denominator of a reduced rational function, it has since been a key notion in several algorithmic developments.

Most of existing algorithms for rational and hypergeometric indefinite summation [2, 5, 3] exhibit dependency of the running time on the value of the dispersion which makes them unnecessarily slow for the cases of large dispersion and small output size (one exception is an algorithm from [4], see also [6] for details).

We analyze the relation between value of the dispersion and running time complexity of indefinite summation algorithms for different classes of summands, and show that the dependency of the running time on dispersion is non-essential (i.e. it is a feature of algorithms, not of the summation problems) in many cases. This leads to practical improvements of the algorithms for indefinite summation, based on ideas of direct indefinite summation [6]. Implementations of those improvements in Maple will be compared to standard Maple summation tools.

References

[1] S. A. Abramov. The summation of rational functions. *Ž. Vyčisl. Mat. i Mat. Fiz.*, 11:1071–1075, 1971.

[2] S. A. Abramov. Indefinite sums of rational functions. In *Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation*, ISSAC '95, pages 303–308, New York, NY, USA, 1995. ACM.

[3] S. A. Abramov and M. Petkovšek. Rational normal forms and minimal decompositions of hypergeometric terms. *Journal of Symbolic Computation*, 33(5):521–543, 2002. Computer algebra (London, ON, 2001).

[4] J. Gerhard, M. Giesbrecht, A. Storjohann, and E. V. Zima. Shiftless decomposition and polynomial-time rational summation. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, pages 119–126 (electronic), New York, 2003. ACM.

[5] R. W. Gosper, Jr. Decision procedure for indefinite hypergeometric summation. *Proc. Nat. Acad. Sci. U.S.A.*, 75(1):40–42, 1978.

[6] E. V. Zima. Accelerating indefinite summation: Simple classes of summands. *Mathematics in Computer Science*, 7(4):455–472, 2013.

Applied and Computational Algebraic Topology

Session Organizers

Graham Ellis
School of Mathematics
National University of Ireland, Galway
graham.ellis@nuigalway.ie

Marian Mrozek
Institute of Computer Science and Computational Mathematics Jagiellonian University
mrozek@ii.uj.edu.pl

Aniceto Murillo
Departamento de Algebra, Geometría y Topología
Universidad de Malaga
aniceto@uma.es

Pedro Real
Institute of Mathematics (IMUS)
Dept. of Applied Mathematics I
University of Seville
real@us.es

Eduardo Saenz de Cabezón
Mathematics and Computation
Universidad de La Rioja
eduardo.saenz-de-cabezon@unirioja.es

Overview

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

Fast computation of Betti numbers on three-dimensional cubical complexes

Aldo Gonzalez-Lorenzo[1,2], Alexandra Bac[1], Jean-Luc Mari[1], Pedro Real[2]

[1] *Aix Marseille Université, CNRS, LSIS UMR 7296,13397, Marseille (France)*
[2] *University of Seville, Institute of Mathematics IMUS, Seville (Spain)*

We introduce a fast and simple method for computing the Betti numbers of a three-dimensional cubical complex. It differs from the incremental algorithm found in [2] in that no cycle detection is needed. Let us remark that this can be applied to compute the Betti numbers of a binary 3D volume [1].

The method is based on the Alexander duality and the Euler-Poincaré characteristic. Given K a cubical complex of dimension 3, $\bar{K} = S^3 \setminus K$, then

$$H_2(K) \cong H^0(\bar{K}) \cong H_0(\bar{K}). \tag{1}$$

Thus, the Betti numbers of dimension 0 and 2 can be computed only by detecting the number of connected components of K and $\bar{K}$. Moreover, the following property of the Euler-Poincaré characteristic is well known:

$$\chi(K) = \beta_0 - \beta_1 + \beta_2 \tag{2}$$

So the 1-Betti number can be deduced from β_0, β_2 and $\chi(K)$, which is easily computed.

The main difficulty lays in the description of $\bar{K} = S^3 \setminus K$, but this is easy in the context of cubical complexes regarding the Khalimsky coordinates of the cells present in the complex. The complexity of this algorithm depends on the size of the bounding box of every connected component.

References

[1] Aldo Gonzalez-Lorenzo, Alexandra Bac, Jean-Luc Mari and Pedro Real, *Cellular Skeletons: a New Approach to Topological Skeletons with Geometric Features*, preprint (2015).

[2] Cecil Jose A. Delfinado and Herbert Edelsbrunner, *An Incremental Algorithm for Betti Numbers of Simplicial Complexes*, Proceedings of the Ninth Annual Symposium on Computational Geometry San Diego, CA, USA, May 19-21, 1993, pp. 232–239.

COMPUTING THE HOMOLOGY OF THE LCM-FILTRATION OF A MONOMIAL IDEAL

FATEMEH MOHAMMADI, ANA ROMERO, EDUARDO SÁENZ-DE-CABEZÓN,
AND HENRY WYNN

Given a monomial ideal $I = \langle m_1, \ldots, m_r \rangle$, we can define a filtration $I = I_1 \supseteq I_2 \supseteq \cdots \supseteq I_r$ where $I_i = \langle m_\sigma | \sigma \subseteq \{1, \ldots, r\} \rangle$ and $m_\sigma = \mathrm{lcm}(m_i | i \in \sigma)$. We call this the lcm-filtration of I. We define the homology of this filtration in terms of the homology of the induced filtrations of the (upper and lower) Koszul simplicial complexes associated to I and to each of the ideals I_i in the filtration.

This homology gives a finer homological description of the structure of the ideal I than the one given by the (multigraded) Betti numbers of I.

We illustrate this new concept by actual computations of some examples using a computer algebra system.

Estimating the position of the mandibular canal in dental radiographs using the generalized Hough transform

D.M. Onchis[1], S.L. Gotia[2], P. Real[3]

[1] *Faculty of Mathematics, University of Vienna, Austria, darian.onchis@univie.ac.at*
[2] *Department of Physiology, Victor Babes University of Medicine and Pharmacy, Timisoara, Romania, lauragotia@yahoo.com*
[3] *Department of Applied Mathematics I, University of Seville, Spain, real@us.es*

In this work, the generalised Hough transform or GHT is used to detect the mandibular canal in dental panoramic radiographs. The method is based on template matching using the fact that the shape of the mandibular canal is usually the same. The proposed procedure consists in an detailed description for the shape of the canal in its canonical form and on preserving topological information before applying incrementally the extraction algorithm. The procedure is robust to recognition under occlusion and to the presence of additional structures e.g. teeth, projection errors.

From a clinical point of view, the marking of the mandibular canal is useful in detecting the nerve for inferior teeth called inferior dental nerve which is found inside it. The position from where we begin our search is given by medical indications as follows: the canal starts at the mandibular foramen in the middle part of the vertical ramus. It continues through the mandibular bone and ends in the menton foramen between apexes of the two inferior premolars.

Any surgical intervention in the mandibular area must prevent any nerve injury. The injury of the nerve would result in prolonged local and lower lip anesthesia for a minimum period of six weeks. Estimating the position of the mandibular canal means knowing the position of the nerve and by this the surgeon can estimate the risks and to adapt the surgical procedure to the individual case.

References

[1] D. Ballard, *Generalizing the Hough Transform to Detect Arbitrary Shapes*, Pattern Recognition, Vol.13, No.2, p. 111-122, 1981.

[2] D. Ciresan, D. Damian, *Preserving topological information in the windowed hough transform for rectangle extraction* In Proceedings of the 28th conference on Pattern Recognition (DAGM'06), Springer-Verlag, Berlin, Heidelberg, p. 172-181, 2006.

[3] J.A. Heather, X. D. Yang, *Spatial Decomposition of the Hough Transform*, The 2nd Canadian Conference on Computer and Robot Vision, 2005.

[4] A. A. Kassim, T. Tan, K. H. Tan, *A comparative study of efficient generalised Hough transform techniques*, Image and Vision Computing, Volume 17, Issue 10, Pages 737-748, August 1999

[5] D.M. Onchis, S.L. Gotia, *Enhancing Dental Radiographic Images in Spline-Type Spaces*. SYNASC 2014: 559-564

[6] L. Xu, E. Oja, P. Kultanen. *A new curve detection method: randomized Hough transform (RHT)*, Pattern Recognition Lett., 11(5), p. 331 - 338, 1990.

Algebraic-topological invariants for combinatorial multivector fields [1]

M. Mrozek[1]

[1] *Jagielloniam University in Krakow, Poland,*

1 Introduction.

In late 90' Robin Forman [2, 3] introduced the concept of a combinatorial vector field on a CW complex, introduced the concept of a chain recurrent set and proved Conley type generalization of Morse inequalities for basic sets consisting of critical cells and periodic trajectories. Conley theory [1] is a generalization of Morse theory to the setting of non-necessarily gradient or gradient-like flows on locally compact metric spaces. In this theory, the concept of a critical point is replaced by a more general concept of an isolated invariant set and the Morse index of a critical point by the Conley index of an isolated invariant set.

Combinatorial vector fields seem to be a natural tool for a coincise approximation and description of the dynamics of differential equations and more generally flows. For instance, given a cubical grid on the plane and a planar vector field, it is natural to set up arrows in the comibinatorial setting of the grid by taking averages of the vectors in the vector field along the one-dimensional faces of the grid. Unfortunately, in most cases this does not meet the requirements of the classical Forman theory that the combinatorial vectors together with the critical cells have to constitute a partition (see Fig. 1).

Recently, T. Kaczynski, M. Mrozek and Th. Wanner [4] defined the concept of an isolated invariant set and the Conley index in the case of a combinatorial vector field on the collection of simplexes of a simplicial complex. The aim of the work announced in this note is to combine the ideas of Forman with some classical concepts of topological dynamics in order to obtain a tool for combinatorization of classical dynamics. In particular, in order to overcome the mentioned limitations of combinatorial vector fields in the approximation of differential equations we introduce combinatorial multivector fields, a generalization of Forman's combinatorial vector fields. We extend the concepts of isolated invariant set and Conley index introduced in [4] to combinatorial multivector fields. Furthermore, we define attractors, repellers, Morse decompositions and present Morse inequalities for such Morse decompositions. These ideas are novel not only for combinatorial multivec-

[1] Research partially supported by the TOPOSYS project FP7-ICT-318493-STREP

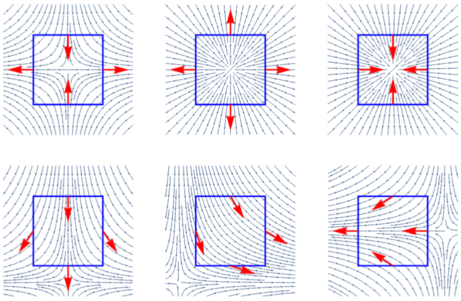


Figure 1: Out of the six examples of averaging a smooth vector field along the one-dimensional faces of a cubical grid only the top middle and bottom left satisfy the partition requirement of a combinatorial vector field of Forman.

tor fields but even for combinatorial vector fields.

2 Combinatorial multivector fields and the Conley index.

Let M denote a finite, regular CW complex and let X be the collection of its cells. In this note it is convenient to identify the collection A of cells with the union $\bigcup A$. In particular, we say that A is closed (open) if A as the union of its cells is closed (open) in M and we write $\operatorname{cl} A$ meaning, depending on the context, either the closure of $\bigcup A$ or the collection of cells in this closure. We use this convention in the following definitions. The mouth of A is $\operatorname{mo} A := \operatorname{cl} A \setminus A$. The collection of cells A is *proper* if $\operatorname{mo} A$ is closed. By the homology of a proper A, denoted $H(A)$, we mean the relative homology $H(A) := H(\operatorname{cl} A, \operatorname{mo} A)$. The respective kth Betti number of A is denoted by $b_k(A)$ and $p_A(t) := \sum b_k t^k$ stands for the associated Poincaré polynomial.

A *multivector* is a proper subset $V \subset X$ admitting a unique cell of maximal dimension. We say that a multivector is *regular* if its homology is zero. Otherwise it is called *critical*. A multivector V is a *vector* if $\operatorname{card} V \leq 2$.

A *multivector field on* X is a partition $\mathcal{V}$ of X into multivectors. A multivector field on X is a *vector field* if each multivector is a vector. It is not difficult to verify that our concept of a vector field on X in the setting of simplicial complexes is in one-to-one correspondence with Forman combinatorial vector field (see [3]).

For each cell $x \in X$ we denote by $[x]_{\mathcal{V}}$ the unique set in $\mathcal{V}$ to which x belongs. We also write $x^\star := [x]^\star_{\mathcal{V}}$. We associate with $\mathcal{V}$ a multivalued map $\Pi_{\mathcal{V}} : X \rightrightarrows X$

given by

$$\Pi_{\mathscr{V}}(x) := \begin{cases} \{x^\star\} & \text{if } x \neq x^\star, \\ \operatorname{cl} x \setminus [x]_{\mathscr{V}} & \text{if } x = x^\star \text{ and } [x]_{\mathscr{V}} \text{ is regular,} \\ \operatorname{cl} x \setminus [x]_{\mathscr{V}} \cup \{x^\star\} & \text{if } x = x^\star \text{ and } [x]_{\mathscr{V}} \text{ is critical.} \end{cases}$$

From now on we fix a combinatorial multivector field $\mathscr{V}$ and we assume that X is invariant with respect to $\mathscr{V}$. A map $\varphi : \mathbb{Z} \nrightarrow A \subset X$ is a *solution* of $\mathscr{V}$ in A thorugh $x = \varphi(0)$ if $\varphi(i+1) \in \Pi_{\mathscr{V}}(\varphi(i))$ for $i, i+1 \in \operatorname{dom} \varphi$. We say that $A \subset X$ is *$\mathscr{V}$-compatible* if $x \in A$ implies $[x]_{\mathscr{V}} \subset A$ for $x \in X$. We say that a proper $S \subset X$ is an *isolated invariant set* if for every $x \in S$ there exists a solution through $x^\star$ in the maximal $\mathscr{V}$-compatible subset of S.

A pair $P = (P_1, P_2)$ of closed subsets of X is an *index pair* for S iff the following three conditions are satisfied

$$x \in P_2,\ y \in P_1 \cap \Pi_{\mathscr{V}}(x) \ \Rightarrow\ y \in P_2, \tag{1}$$

$$x \in P_1,\ \Pi_{\mathscr{V}}(x) \setminus P_1 \neq \emptyset \ \Rightarrow\ x \in P_2, \tag{2}$$

$$S = \operatorname{Inv}(P_1 \setminus P_2). \tag{3}$$

We say that the index pair P is *saturated* iff $P_1 \setminus P_2 = S$.

Theorem 2.1 *Given an isolated invariant set S, the pair* $(\operatorname{cl} S, \operatorname{mo} S)$ *is a saturated index pair for S. If P and Q are index pairs for S, then* $H(P_1, P_2)$ *and* $H(Q_1, Q_2)$ *are isomorphic. In particular* $H(S) = H(\operatorname{cl} S, \operatorname{mo} S)$*.*

Theorem 2.1 allows us to define the *homology Conley index* of S as $H^\kappa(P_1, P_2) = H^\kappa(P_1 \setminus P_2)$ for any index pair P of S. Note that in the combinatorial setting of this paper, the Conley index of an isolated invariant set S coincides with $H(S)$.

3 Morse inequalities.

We say that a $\mathscr{V}$-compatible $N \subset X$ is a *forward trapping region* if $\Pi_{\mathscr{V}}(N) \subset N$. We say that A is an *attractor* if there exists a trapping region N such that $A = \operatorname{Inv} N$. In a dual way we define a *backward trapping region* and a repeller.

Theorem 3.1 *A subset* $A \subset X$ *is an attractor (repeller) if and only if A is isolated invariant, closed and a forward (backward) trapping region.*

Let $\rho : \mathbb{Z} \to X$ be a full trajectory and let $\operatorname{im}^k \rho$ denote the set $\{\rho(i) \mid i \geq k\}$. Define $\omega(\rho)$, the *ω limit set of* ρ as the intersection of maximal invariant subsets

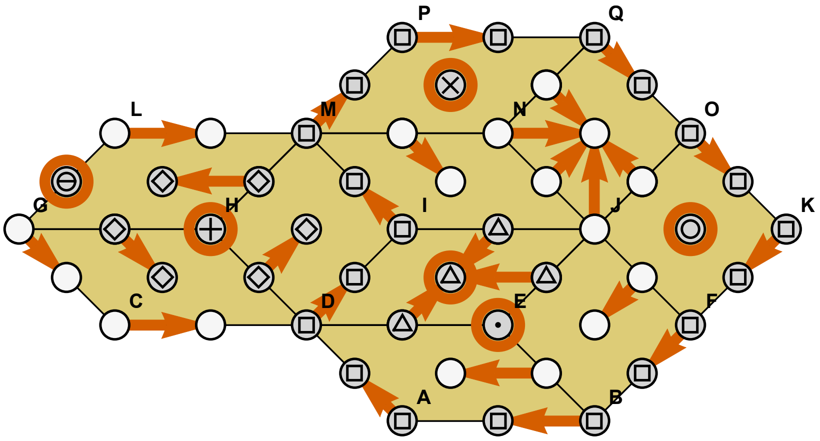


Figure 2: A Morse decomposition. The cells in the same Morse set are denoted by a common symbol.

of $\mathscr{V}$-compatible coverings of $\operatorname{im}^k \rho$ taken over all positive k. In a dual way define $\alpha(\rho)$, the *α limit set of ρ*.

Let $\mathbb{P}$ be a finite set. The collection $\mathscr{M} = \{M_p \mid p \in \mathbb{P}\}$ is called a *Morse collection of X* if M_p are mutually disjoint, isolated invariant subsets of X, for every solution φ there exist $p, p' \in \mathbb{P}$ such that $\alpha(\varphi) \subset M_{p'}$, $\omega(\varphi) \subset M_p$, and if for a solution φ and $p \in \mathbb{P}$ we have $\alpha(\varphi) \cup \omega(\varphi) \subset M_p$, then $\operatorname{im}\varphi \subset M_p$.

Let $\leq$ be a partial order on $\mathbb{P}$. We say that $\leq$ is *admissible with respect to $\mathscr{M}$* if for every full solution φ the $p, p' \in \mathbb{P}$ in the definition of the Morse collection satisfy $p \leq p'$. The Morse collection $\mathscr{M}$ is called a *Morse decomposition of X* if such an admissible partial order exists. Note that the intersection of admissible orders is an admissible order and any extension of an admissible order is an admissible order. In particular, every Morse decomposition has a minimal admissible order as well as an admissible linear order.

Theorem 3.2 *Given a Morse decomposition $\mathscr{M} = \{M_p \mid p \in \mathbb{P}\}$ of an isolated invariant set S we have*

$$\sum_{p\in\mathbb{P}} p_{M_p}(t) = p_S(t) + (1+t)q(t) \tag{4}$$

for some non-negative polynomial q. In particular, if $m_k(\mathscr{M}) := \sum_{p\in\mathbb{P}} b_k(M_p)$,

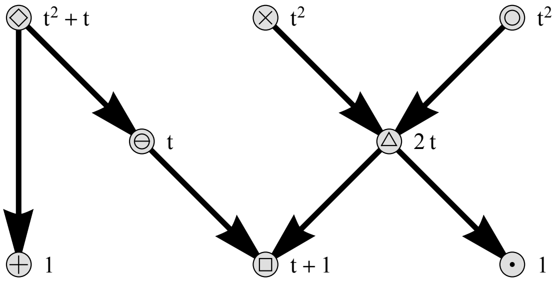


Figure 3: Poincaré polynomials and the minimal admissible order of the Morse decomposition in Figure 2.

then for for any $k \in \mathbb{Z}^+$ we have

$$\begin{aligned} m_k(\mathscr{M}) - m_{k-1}(\mathscr{M}) + \cdots \pm m_0(\mathscr{M}) &\geq b_k(S) - b_{k-1}(S) + \cdots \pm b_0(S), \\ m_k(\mathscr{M}) &\geq b_k(S). \end{aligned}$$

Figure 2 presents a CW complex X with a combinatorial multivectors field. Each cell of the CW complex is identified with a small circle in its center of mass. The combinatorial multivector field is denoted by arrows going from each cell x to $x^\star$. Critical cells are denoted by a ring. The figure also marks a Morse decomposition

$$\mathscr{M} = \{M_+, M_\Diamond, M_\ominus, M_\Box, M_\times, M_\triangle, M_\cdot, M_\circ\}$$

consisting of 8 Morse sets. The respective Poincaré polynomials together with the minimal admissible order are presented in Figure 3. The resulting graph is known as the Morse-Conley graph of the Morse decomposition. It provides a concise characteristic description of the dynamics and may serve as a classification tool in the qualitative study of dynamical systems.

References

[1] C. Conley. *Isolated Invariant Sets and the Morse Index*, Amer. Math. Soc., CBMS Regional Conf. Series Math. **38**, 1978.

[2] R. Forman, Morse theory for cell complexes, *Adv. Math.* **134**(1998), 90–145.

[3] R. Forman, Combinatorial vector fields and dynamical systems, *Math. Z.* **228**(1998), 629–681.

[4] T. Kaczynski, M. Mrozek, Th. Wanner. Towards a Formal Tie Between Combinatorial and Classical Vector Field Dynamics, *IMA Preprint Series* #2443, November 2014.

Persistence over a topos of variable sets.

J. Pita Costa[1], M. Vejdemo Johansson[1], P. Škraba[2]

[1] *Laboratory of Artificial Intelegence, Inštitut Jozef Štefan, Slovenia,*
{joao.pitacosta,primoz.skraba}@ijs.si
[2] *Computer Vision and Active Perception Laboratory, KTH Royal Institute of Technology, Sweden,*
mvj@kth.se@wlu.ca

The basic technique of standard persistent homology identifies a global structure by inferring high-dimensional structure from low-dimensional representations and studying properties of a continuous space by the analysis of a discrete sample of it, assembling points into global structure. It is formalised with several different approaches to the underlying algebraic structures: persistence modules have been defined as graded modules over $k[t]$, or as graded modules over a quiver of type A_n. Each of these formalisations have brought extensions of both algorithmics and the scope of what TDA methods can be envisioned and studied. An alternative to set theory for the foundation of Mathematics based on topoi (i.e., cartesian closed categories with enough structure to produce a classifier of subobjects for each object) was proposed in [3] providing effective means for transferring results and techniques between distinct fields, as in [6].

The idea of applying sheaves to encode the shape of persistent homology is not itself new [5]. The novelty of our approach is to consider a topos theoretic approach to set theory permitting ideas like time variable sets and provides tools to consider such a common framework, an appropriate approach to generalise a time-driven theory such as persistence. In this topos-based approach, persistent homology is computed from the internal homology of simplicial complexes over a set theory in which elements have encoded lifetimes. In such a setting, a filtered topological space corresponds to a topological space where parts of the space come in at later times; the construction of the homology functor immediately provides homology groups where elements come in and go away as time flows. This leads to a formulation in the topos setting for the various flavours of persistence that have emerged so far: standard, multi-dimensional and zigzag persistence. For each of these cases, the recognition of an underlying algebraic structure has contributed both to the identification of new problems and to the development of new algorithms [4].

Persistence permutes the encoding of topological features by multisets of pairs of real numbers called *persistence diagrams*, where the birth and death time of every connected component of the sample of a given topological space is recorded. Each element of one persistence diagram corresponds to a basis element of the correspondent module. For a given time point t, we can determine the local Betti number at t by counting the number of points (b,d) in the multiset such that $b \leq t \leq d$. This can be visualized either as counting points in a quadrant or as counting bars intersecting a vertical line. There is nothing that keeps us from doing this for longer spans of query time intervals – we can ask for points (b,d) such that $b \leq x \leq y \leq d$ for some interval (x,y). This produces Betti numbers that persist for *at least* the time period (x,y).

The set of points of all such diagrams determines a complete Heyting algebra that can explain aspects of the relations between correspondent persistence bars through the algebraic properties of its underlying lattice structure. The category of sheaves over this Heyting algebra constitutes a topos, behaving as a category of sheaves of sets over a topological space. In line with [8] and motivated by [1], we consider the topos of sheaves over the algebra of lifetimes $\mathscr{L}$, denoted by $[\mathscr{L}^{op}, Set]$, established in [7]. We explore a topos-based approach to foundations for persistent homology. We will show that the considered topos exhibits the same features we are expecting from a persistent topology. Within the set theory of this topos, we can develop semi-simplicial sets, chain complexes, and a combinatorial homology theory that reimplements classical persistent homology by introducing the persistence aspects already at the level of set theory. We shall also consider the representation of this category in Vect, its relation with the generalised persistence modules from [2], and discuss theorems that permit us a step forward towards stability results that can be reached at the underlying algebra level. Finally, we describe some ideas on how a choice of a different base Heyting algebra can generate other shapes of a persistence theory, thus potentially unifying multidimensional, tree-based, DAG-based and zig-zag persistence under a common foundation.

References

[1] M. Barr and C. Wells. *Category theory for computing science*, Michael Barr and Charles Wells (1995).

[2] P. Bubenik, Vin de Silva, and J. Scott. *Metrics for generalized persistence modules*, arXiv:1312.3829 (2013).

[3] O. Caramello. *The unification of Mathematics via Topos Theory*, arXiv:1006.3930 (2010).

[4] G. Carlsson. *Topology and data*, Bulletin-American Mathematical Society **46**, pp. 1–54 (2009).

[5] J. Curry. *Sheaves, Cosheaves and Applications*, PhD thesis, University of Pennsylvania (2013).

[6] C. Flori. *A first course in topos quantum theory.* Springer (2013).

[7] J. Pita Costa, M. Vejdemo-Johansson and P. Škraba. *Variable sets over an algebra of lifetimes: a contribution of lattice theory to the study of computational topology*, arXiv:1409.8613 (2014).

[8] M. Vejdemo-Johansson. *Sketches of a platypus: persistent homology and its algebraic foundations*, Algebraic Topology: Applications and New Directions, pp. 295–320 (2014).

Fast and Stable Topological Profiles of Noisy 2D Images

V. Kurlin[1],

[1] *Microsoft Research Cambridge and Durham University, UK; vitaliy.kurlin@gmail.com*

This is a short abstract for an extended version of the conference paper [6]. The full version with a C++ code will be at author's website `http://kurlin.org` in late June 2015. The original 6-page paper [6] describes a persistence-based approach to predicting the number of holes in a 2D shape given by a noisy sample of points without any extra parameters such as a scale α or a noise bound ε.

A *shape* X is any compact subset of the plane. A *hole* is any bounded connected component in the complement of X in the plane. The *α-offset* X^α is the set of points at a distance not more than α from X. An *ε-sample* of X is a finite cloud C of points such that $X \subset C^\varepsilon$ and $C \subset X^\varepsilon$. We summarise below the past work [6].

(1) The input is a 2-dimensional cloud C of n points with any real coordinates.

(2) The output is the probability distribution for the number of holes in the α-offsets C^α when the scale α is uniformly distributed between natural bounds.

(3) The holes are traced from their birth to death by computing the 1D persistence diagram for the filtration (nested sequence) of α-offsets C^α (or α-complexes).

(4) The 1D persistence is found in time $O(n \log n)$ by building the Delaunay triangulation on the cloud C and using the duality between cycles in C^α and components of the complement of C^α in the plane for maintaining a union-find structure [1].

(5) We proved that for a dense sample C of a good shape X (with holes of comparable sizes) the algorithm finds the true number of holes in X using only C.

Here are the improvements of the extended version in comparison with [6].

(6) The algorithm now accepts any real image and extracts a point cloud using a Canny edge detector [4], which allows a user to tune a threshold for edge points.

(7) A cloud C was assumed to be a sample of a connected shape X in [6]. We now split a cloud C of edge points from an image into clusters to analyze each cluster.

(8) The bounded noise model [6] is replaced by the *distance to measure* approach [3], which filters outliers using a number k of close neighbors. Instead of α-complexes filtering a Delaunay triangulation we compute the 1D persistence for the filtration of subcomplexes in the *power diagram* on weighted points [2]. The weight of each point is proportional to an average distance to k nearest neighbors.

(9) The 1D persistence diagrams for filtrations of the power diagrams on all clusters of C are combined into a topological profile of the original image, which will be stable under perturbations of a given point cloud, also for noise with outliers.

(10) We include experiments on the Berkeley segmentation dataset BSD 500 so that the topological profiles can be used as new features in object recognition.

(11) We extend guarantees from [6] to a larger class of 2D shapes X with holes of any topological form so that new holes can be born in X^{α} when α is increasing.

(12) The original Java implementation is turned into a clean C++ code using CGAL [5], which will be publicly available at author's website `http://kurlin.org`.

References

[1] Attali, D., Glisse, M., Hornus, S., Lazarus, F., Morozov, D., *Persistence-sensitive simplification of functions on surfaces in linear time*, in *Topological Methods in Visualization* (TopoInVis), Snowbird, USA (2009).

[2] F. Aurenhammer *Power diagrams: properties, algorithms and applications*, SIAM J. Comput., **16**, 78–96 (1987).

[3] M. Buchet, F. Chazal, T. K. Dey, F. Fan, S. Oudot, Y. Wang, *Topological analysis of scalar fields with outliers*, in *Proceedings of Symposium on Computational Geometry*, (SoCG 2015).

[4] J. Canny, *A computational approach to edge detection*, IEEE Transactions on Pattern Analysis and Machine Intelligence, **8**, pp. 679–698 (1986).

[5] *CGAL library*, `http://doc.cgal.org/4.2/CGAL.CGAL/html/packages.html`.

[6] V. Kurlin, *A fast and robust algorithm to count topologically persistent holes in noisy images*, in *Proceedings of Computer Vision and Pattern Recognition* (CVPR), Columbus, USA, pp. 1458–1463 (2014). The longer unpublished 10-page version is arXiv:1312.1492.

Using persistent homology to reveal hidden information in place cells

Gard Spreemann[1], Benjamin Dunn[2], Magnus Botnan[1], Yasser Roudi[2], Nils Baas[1]

[1] *Department of Mathematical Sciences, Norwegian University of Science and Technology, Trondheim, Norway, {spreeman,botnan,baas}@math.ntnu.no*
[2] *Kavli Institute for Systems Neuroscience, Norwegian University of Science and Technology, Trondheim, Norway, {benjamin.dunn,yasser.roudi}@ntnu.no*

Mammalian hippocampi contain *place cells*, which are nerve cells that respond preferentially when the animal is in distinct regions of space [1]. These regions of elevated activity of the cells, their *place fields*, can be thought of as constituting a cover of the animal's spatial environment, and so suggest a connection to topology.

Neuroscientists are able to record simultaneously the firing events for hundreds of place cells as a rat navigates space, and it is reasonable to believe that the pairwise correlations of these *spike trains* are a good proxy for the degree of intersection of the place fields. Therefore, the flag complex of the associated correlation graph should be a filtered simplicial complex that approximates the homotopy type of the spatial environment. Indeed, it has been demonstrated [2, 3] that under certain simple models for neuron activity, persistent homology can accurately recover the homology of the spatial environment in this way.

It was shown already in [1] that place cell activity correlate not just with spatial position, but also with activities such as eating, drinking, sleeping, biting, and with a variety of sensory inputs, such as head orientation, smell and visual cues. Recent work [4] has demonstrated how persistent homology can help determine whether the (partly unknown) data encoded by place cells is geometric in nature or not.

Our work, which utilizes techniques similar to [3, 4], is concerned with an animal that explores a path α on a configuration manifold M. This a priori unknown manifold is assumed to be a product of simple factors (intervals, circles, spheres, etc.), and each place cell has associated to it a point $p \in M$. Neuron firing probability is then assumed to descrease monotonically as a function of a certain distance between $\alpha(t)$ and p. If, for example, the spatial environment is a box I^2, and place cells fire solely based on *position* and *head direction*, then $M = I^2 \times S^1$. In this case firing probabilities are governed by sums of distances in I^2 and distances in S^1.

We suppose we are given a list of candidate stimuli (candidate factors of M) that the neuroscientist believes governs place cell firing, together with experimentally obtained spike trains $s_1, \dots, s_N$ for a population of N neurons, as well as samples $\alpha(t_1), \dots, \alpha(t_T) \in M$ of the animal's path through configuration space. By assuming the neural activity to be governed by a kinetic Ising model (as is common, see e.g. [5, 6]), we can use likelihood maximization to determine the contribution of various factors of M to the observations $s_1, \dots, s_N$. The contributions of these stimuli can then be removed, leaving residuals with which the same process as for proper spike trains is repeated. Persistent homology can then inform us as to whether any homological information is left; in particular, if the list of candidate stimuli has been exhausted and non-trivial homology remains, the researcher will have gained valuable insight into the nature of hidden data encoded by the neurons.

Returning to the simple example of $M = I^2 \times S^1$, one might imagine that the researcher knows only about spatial stimulus, and that he is unaware that also head direction influences firing. He therefore hypothesizes that $M = I^2$, and performs an experiment recording spike trains and the rat's trajectory through I^2. After inferring away the spatial position's contribution to the firing events, and computing persistent homology of the residual "spike trains", he observes a persistence diagram that (1) is highly incompatible with random data, and (2) has non-trivial first homology. From 1, the researcher gets a strong indication that spatial preference is insufficient to explain his firing data. This may well have been learned from the likelihood itself, or from spectral analysis of the correlations. Observation 2, however, tells him that the unknown stimulus is circular in nature, and thus guides his further investigations.

In various simulated settings with a range of stimuli — position, direction of (multiple) head(s), neuron couplings, θ-wave phase preference — we are able to carry out the process described above with a high degree of success, indicating that our method may provide useful information also when applied to real experimental data.

We also believe our method is applicable to a wider range of problems wherein one's data consists of events from a Bernoulli process with probabilities given as monotonic functions of distances on an unknown manifold.

References

[1] J. O'Keefe and J. Dostrovsky, *The hippocampus as a spatial map. Preliminary evidence from unit activity in the freely-moving rat*, Brain research **34**, 1, pp. 171–175 (1971).

[2] C. Curto and V. Itskov, *Cell groups reveal structure of stimulus space*, PLoS Computational Biology **4**, 10 (2008).

[3] Y. Dabaghian, F. Mémoli, L. Frank and G. Carlsson, *A Topological Paradigm for Hippocampal Spatial Map Formation Using Persistent Homology*, PLoS Computational Biology **8**, 8 (2012).

[4] C. Giusti, E. Pastalkova, C. Curto and V. Itskov, *Clique topology reveals intrinsic geometric structure in neural correlations*, arXiv:1502.06172 [q-bio.NC] (2015).

[5] Y. Roudi and J. Hertz, *Mean Field Theory for Nonequilibrium Network Reconstruction*, Physical review letters **106**, 4 (2011).

[6] Y. Roudi, B. Dunn and J. Hertz, *Multi-neuronal activity and functional connectivity in cell assemblies*, Current Opinion in Neurobiology **32**, pp. 38–44 (2015).

Persistence of generalized eigenspaces of self-maps

H. Edelsbrunner[1], G. Jablonski[2], M. Mrozek[3]

[1] *IST Austria, Klosterneuburg*
[2] *Jagiellonian University, Poland, grzegorz.jablonski@uj.edu.pl*
[3] *Jagiellonian University, Poland*

My talk is divided into two parts: first I summarize results which are described in [3]. This includes definitions and basic algorithms to compute persistence of eigenspaces of maps induced in homology. The second part of the talk is about the progress in computation of generalized eigenspaces of maps.

In the classical persistent homology one analyses given filtration of topological space X. Such a filtration is defined as sequence of nested subspaces $\emptyset = X_0 \subset X_1 \subset X_2 \subset ... \subset X_n = X$. One examines how group of homology changes in the filtration, especially when cycles appear and disappear. Cycles that survive longer in the filtration are more important than the other ones [2]. As a consequence we can pick up only crucial information and remove cycles that come from noise.

In the persistent homology for a maps we work on a point cloud data S from a topological space $X \subset \mathbf{R}^k$ and an approximation of a map $f : X \to X$ given by $g : S \to S$.

We define Vietoris-Rips complex $R_\varepsilon(S)$ on a set of points S for a parameter $\varepsilon \in \mathbf{R}$ [4, Chapter III.2] as a simplicial complex s.t. simplex $\sigma \in R_\varepsilon$ if the pairwise distances between vertices of σ are smaller than ε. For simplicity we denote $R_{\varepsilon_i}(A)$ as $R_i(A)$ for any set of points X.

Therefore, a sequence $\varepsilon_0 < \varepsilon_1 < .. < \varepsilon_n$, where $\varepsilon_i \in \mathbf{R}$ induces the filtration:

$$R_0(S) \subset R_1(S) \subset \ldots \subset R_n(S) \tag{1}$$

We use the notation $H_*(X)$ for the homology of a space X and f_* for the homology of a map f. We would like to study the function $f_* : H_*(X) \to H_*(X)$ using information from g. In [3] we were interested in eigevalues and eigenvectors of f_*. It is not possible to define f_* on the presented filtration if the map is expansive. It is a consequence of the fact that not all images of simplices from $R_i(S)$ under the simplicial map induced by g lie in $R_i(S)$. To compute eigenvectors for an eigenvalue λ, we use the graph of the function g. The set $G \subset S \times S$, where $(x, g(x)) \in G$ for all $x \in S$ is the graph of g. We define two projections $p, q : R_i(G) \to R_i(S)$ on the first and second coordinate respectively. We get two linear maps $p_* : H_*(R_i(G)) \to H_*(R_i(S))$ induced by p and $q_* : H_*(R_i(G)) \to H_*(R_i(S))$ induced by q. Coefficients used to compute homology groups come from closed field, so homology groups are vector spaces. Using this construction we can compute eigenvectors for a chosen eigenvalue λ as vectors $v \in H_*(R_i(G))$ fulfilling the equation:

$$\lambda p_*(v) = q_*(v). \tag{2}$$

The generalized eigenvectors for a map $\alpha : A \to A$ are vectors $v \in A$ such that:

$$(\alpha - id)^k(v) = \lambda v \tag{3}$$

where $k \in \mathbf{N}$, id is the identity function and $(\alpha - \mathrm{id})^k$ is k-fold composition of $\alpha - \mathrm{id}$ with itself. In the talk I would like to present the ideas how to extend the notion of generalized eigenspaces for pairs of of projections. Specifically, I show that the elements of recursively defined sets:

$$\begin{aligned} E_1 &= \{v : \lambda p_*(v) = q_*(v)\} & (4) \\ E_m &= \{v : (\lambda p_* - q_*)(v) \in p(E_{m-1})\} & (5) \end{aligned}$$

are equivalent of generalized eigenvectors for a pair of maps p_*, q_*.

Notice, that for every space of the sequence $R_1(G), \ldots, R_n(G)$ we get set of spaces $E_1, \ldots, E_m$. The idea of persistence for vector spaces was first introduced in [1]. I show how the spaces $E_1, \ldots, E_m$ for different levels can be studied using persistence and algorithms introduced in [3].

This research was supported in part by National Science Centre Poland grant no. DEC-2013/09/N/ST6/02995 and by the TOPOSYS project FP7-ICT-318493-STREP

References

[1] G. Carlsson, V. D. Silva *Zigzag Persistence*, Foundations of Computational Mathematics 10(4): 367-405, Springer New York, 2008.

[2] H. Edelsbrunner, J Harer, *Persistent Homology – a Survey*, Contemporary Mathematics 453: 257-282, 2008.

[3] H. Edelsbrunner, G. Jablonski and M. Mrozek *The Persistent Homology of a Self-map*, Foundations of Computational Mathematics, online first.

[4] H. Edelsbrunner, J. Harer *Computational topology: an introduction*, American Mathematical Soc., 2010.

Algebraic Topology For Unitary Reflection Groups - Scalable Homology Computing

M. Juda[1]

[1] *Jagiellonian University, Poland; mateusz.juda@uj.edu.pl; This research is supported by the Polish NCN under grant 2012/05/N/ST6/03621 and by the TOPOSYS project FP7-ICT-318493-STREP.*

In last few years computational homology lose attention to persistent homology. It is mostly because of practical applications of persistence homology in data analysis. The task of computing homology may be reduced to persistence homology but only over $\mathbb{Z}_2$ coefficients. However, many applications of homology theory require $\mathbb{Z}$ coefficients. It is especially important in computer assisted proofs.

In this talk we show a method for computing homology for large simplicial complexes using parallel shared memory architecture. Our motivation is from pure mathematical problems. Namely, we are interested in posets of eigenspaces of elements of a unitary reflection group, for a fixed eigenvalue. We check if a poset is Cohen-Macaulay, i.e. it has at most top-dimensional reduced homology.

The discrete Morse theory for finite, regular, CW complexes, developed by R. Forman [1] is a powerful reduction method for computing homology [2, 4]. Recall that a *discrete vector field* (DVF) on a regular CW complex X is a matching on the complex facet digraph. Unmatched cells are called *critical cells*. The DVF is *acyclic* if the digraph, with directions reversed on matching edges, is acyclic. Using critical cells of an acyclic DVF on X we can build so called Morse complex. Its homology groups are isomorphic to homology groups of X. We also know that the number of critical cells in dimension d is greater or equal to the complex d-th Betti number (the Morse Inequalities).

For applications it is crucial to get the smallest possible number of critical cells. However, the decision problem is NP-complete. From experiments we know that, in practice, greedy methods behave very well [2]. The methods match elements locally, keeping the total matching acyclic.

Our most challenging data set contains 342921600 simplices in dimension 3. In such scale even building a simplicial complex data structure (generating and linking lower dimensional faces) is time consuming. We need an efficient method for simplicial, non-structured data. There are parallel algorithms available to construct an acyclic DVF, but only for $2D$ and $3D$ structured grids [5]. Currently available algorithms for simplicial and general CW complexes construct the acyclic DVF in single-thread (ST) computations. Assuming enough space in RAM memory the ST methods work for for us. The main problem is that they are very inefficient for currently available multi-core (MC) hardware.

New algorithms implemented in CAPD::RedHom library build an acyclic DVF in parallel for simplicial and Lefschetz complexes. For simplicial data sets we are able to build a data structure also in parallel. Our algorithm for DVF construction uses reduction (elementary collapse) or coreduction pairings. An significant part of the algorithms is that we do not use expensive operations, e.g. atomic variables, code synchronization. We only use well-studied parallel algorithms patterns: sort, prefix sum (scan), reduce. Because of that our algorithms can be implemented in different frameworks easily, e.g TBB, Thrust(GPU CUDA and OpenMP).

In the following table we show experimental results based on our implementation and the huge data set mentioned above. The first two columns show measures for an implementation based on standard approach: processing in a queue, like Breadth-first search algorithm. The third column shows measures for our new algorithm in a ST computations. The last column is also for the the new method but executed in paralell. It is very important that the new method gives us an optimal number of critical cells. In the other cases we need to run another method to compute the homology of the Morse complex. Our implementation of algebraic reductions (KMS method [3]) requires for the computations 2 days. Smith diagonalization is not needed, because the reduced complex is boundaryless. It means that we are able to reduce computation time from more than 2 days to 25 minutes. We performed the computations on the following hardware configuration: 8 Intel(R) Xeon(R) @ 2.67GHz (8 cores each), 512 GB RAM.

	S1 coreduction	S1 reduction	S2 coreduction	Parallel coreduction
cpu user [s]	8748.62	7636.15	9879.01	25121.08
cpu sys [s]	314.44	313.42	378.03	525.3
total cpu [s]	9063.06	7949.57	10257.04	25646.38
Cpu %	99	99	99	1709
elapsed [s]	9073	7953	10285	1500
Memory [GB]	333.48	333.48	333.48	333.48
# 0-Critical cells	1	1	1	1
# 1-Critical cells	0	148	0	0
# 2-Critical cells	1691	975	0	0
# 3-Critical cells	21890412	21889548	21888721	21888721

References

[1] Robin Forman. Morse theory for cell complexes. *Advances in Mathematics*, 134(1):90 – 145, 1998.

[2] S. Harker, K. Mischaikow, M. Mrozek, V. Nanda, H. Wagner, M. Juda, and P. Dłotko. The efficiency of a homology algorithm based on discrete morse theory and coreductions. *published in: Proceedings of the 3rd International Workshop on Computational Topology in Image Context, Chipiona, Spain, November*, pages 41–47, 2010.

[3] T. Kaczynski, M. Mrozek, and M. Slusarek. Homology computation by reduction of chain complexes. *Computers & Mathematics with Applications*, 35(4):59–70, February 1998.

[4] Konstantin Mischaikow and Vidit Nanda. Morse theory for filtrations and efficient computation of persistent homology. *Discrete & Computational Geometry*, 50(2):330–353, 2013.

[5] Nithin Shivashankar and Vijay Natarajan. Parallel computation of 3d morse-smale complexes. *Comp. Graph. Forum*, 31(3pt1):965–974, June 2012.

Computing the persistence of a self-map with the Kronecker canonical form

M. Ethier, G. Jabłoński, M. Mrozek[1]

[1] *Jagiellonian University, Krakow, Poland,*
{marc.ethier, grzegorz.jablonski, marian.mrozek}@uj.edu.pl

This research is supported by the Toposys project FP7-ICT-318493-STREP.

Persistent homology [1] has proved in the last two decades to be a very useful tool in several branches of applied mathematics and computer science. In [2], a novel application of persistence to the computational analysis of dynamical systems is introduced. Given a self-map on a point cloud S obtained by sampling an unknown continuous map $f : X \to X$, one may consider the induced simplicial map over the Vietoris-Rips complex $R_i(S) = R_{\varepsilon_i}(S)$ for a given parameter ε_i, and thence the linear map φ_i induced in the homology $H_*(R_i(S), \mathbf{F})$ over a given field by this simplicial map. Looking at the eigenspace of φ_i for a given value $t \in \mathbf{F}$, one may study its persistence along the Vietoris-Rips filtration. This provides a first step towards understanding the persistence of the self-map, long-lasting eigenvectors being likely to describe its actual dynamical properties.

Since when the self-map is expanding, there is no guarantee that the image of a given simplex by the simplicial map will already be in the Vietoris-Rips filtration at any given step, one may build partial simplicial maps and then use an extension of the previous framework to eigenspaces for pairs of maps defined for $t \in \mathbf{F}$ as

$$E_t(\varphi_i, \psi_i) = \ker(\varphi_i - t\psi_i)/(\ker \varphi_i \cap \ker \psi_i). \tag{1}$$

Here the map ψ_i is induced in homology by the inclusion map between the domain of the partial simplicial map and the Vietoris-Rips complex at step i. The domain and image of φ_i and ψ_i are not necessarily isomorphic. Grzegorz Jabłoński will be recalling this framework in his talk.

It may happen that $E_t(\varphi, \psi)$ be non-trivial for every $t \in \mathbf{F}$, a phenomenon that was termed "abundance of eigenvalues" in [2]. This difficulty in finding the eigenvalues for the pair (φ, ψ), and in identifying them as dynamically significant, raised the question whether there exists a way to build the sequence of eigenspaces, and compute their persistence, for all eigenvalues simultaneously. The correct mathematical structure to study this question is the *Kronecker canonical form* [3, Chapter 12] for $m \times n$ matrix pencils $tB - A$. For every such pencil, there exist invertible matrices $Q \in M^{m\times m}(\mathbf{F})$ and $R \in M^{n\times n}(\mathbf{F})$ such that

$$Q^{-1}(tB - A)R = \operatorname{diag}\{L_{\varepsilon_1}, \ldots, L_{\varepsilon_p}, L^T_{\eta_1}, \ldots, L^T_{\eta_q}, tN - I_q, tI_r - C\} \tag{2}$$

where $0 \leq \varepsilon_1 \leq \varepsilon_2 \leq \ldots \leq \varepsilon_p$, $0 \leq \eta_1 \leq \eta_2 \leq \ldots \leq \eta_q$, the $\varepsilon \times (\varepsilon+1)$ blocks

$$L_\varepsilon = \begin{bmatrix} t & -1 & & \\ & \ddots & \ddots & \\ & & t & -1 \end{bmatrix} \tag{3}$$

are known as *column Kronecker blocks* of *index* ε and the $(\eta+1)\times\eta$ blocks L_η^T as *row Kronecker blocks*, N and C are rational canonical forms with N being in addition nilpotent, and I_q and I_r are identity matrices. The column Kronecker blocks L_ε indicate the existence of polynomial solutions $x(t)$ of degree ε of $(tB-A)\cdot x(t) = 0$ valid for every $t \in \mathbf{F}$, while the eigenstructure of C, known as the *finite eigenstructure* of the pencil, corresponds to eigenvectors belonging to specific eigenvalues. The intuition is that eigenvectors belonging to the finite eigenstructure should correspond to the actual dynamics of the reconstructed self-map, while those coming from column Kronecker blocks are mostly due to noise.

There exist algorithms [4], which I intend to discuss, to extract from a matrix pencil $tB-A$ information about its Kronecker structure, and thence the eigenvectors themselves, preserving the information about whether they belong to the finite eigenstructure or to Kronecker blocks. They allow one to compute the eigenspace $E_t(\varphi,\psi)$ and the generalized eigenspace discussed by Grzegorz Jabłoński in his talk for every field value t simultaneously in a single pass, even for infinite fields such as $\mathbf{Q}$. Writing $E_t(\varphi,\psi)$ as the direct sum of a finite part and a column Kronecker part further allows the latter to be quotiented out in order to concentrate on vectors assumed to truly represent the desired dynamics, thus improving the reconstruction process. We have in addition developed a framework to think of the vectors from the Kronecker part as elements of a space of polynomial functions and therefore compute their persistence independently of given field values. This part of the work is still ongoing, as for now we only understand this framework when working on a finite field, but it should also allow improved understanding of the information we may obtain about a self-map by the reconstruction process.

References

[1] H. Edelsbrunner and J. Harer, *Persistent homology — a survey*, Contemporary Mathematics, **453**, pp. 257–282 (2008).

[2] H. Edelsbrunner, G. Jabłoński and M. Mrozek, *The Persistent Homology of a Self-Map*, Found. Comput. Math., DOI=10.1007/s10208-014-9223-y, 32 p. (2014).

[3] F.R. Gantmacher, *The Theory of Matrices*, Chelsea Publishing Company, New York, 374+276 p. (1959).

[4] P. van Dooren, *The Computation of Kronecker's Canonical Form of a Singular Pencil*, Lin. Alg. Appl., **27**, pp. 103–140 (1979).

EXPLORING RELATIONSHIPS BETWEEN HOMOLOGY GENERATORS USING ALGEBRAIC-TOPOLOGICAL MODELS OF REGULAR CW-COMPLEXES

P. Real[1], A. Gonzalez-Lorenzo[1], A. Bac[2], J.L. Mari[2], D. Onchis-Moaca[3].

[1] *Institute of Mathematics IMUS, University of Seville, Spain real@us.es*
[2] *Aix Marseille Université, CNRS, LSIS UMR 7296, 13397, Marseille (France)*
[3] *Faculty of Mathematics, University of Vienna, Austria.*

Homology information of a geometric space X concerns to processed and structured algebraic data related to homology generators of X and relations between them. An simple example of homology information of a geometric space is provided by the numerical topological invariants called Betti numbers. If X is a regular CW-complex embedded in the euclidean three-dimensional space, Betti numbers β_0, β_1 and β_2 respectively measure the number of different connected components, homological tunnels and cavities of X. Nevertheless, homology information of X is not reduced in general to that provided by Betti numbers. For example, a torus and a three-dimensional sphere with two handles has the same Betti numbers but they are not homologically equivalents. To construct efficient homology information solvers for tessellated domains with finite element or volume meshes can greatly benefit the modeling of devices in electrical and electronic engineering [7], the design of scaffolds and tissues in Computer Aided Tissue Engineering [9] and in generating new applications in Computer Vision and Computer Graphics [8].

Homology operations deals with relationships between homology generators. For example, the cavity (homology generator of dimension two) of a three-dimensional sphere is clearly related in a natural way to the connected component (homology generator of dimension 0) of it. The two tunnels (1-dimensional homology generators) of a three-dimensional torus T are related to the cavity of T (in fact, there is a topological decomposition of the cavity as a "product" of them) and also to the 0-homology generator of T. Some classical homology operations (concretely, Steenrod squares and powers) has been already treated in algorithmic terms and at chain complex level in, for example, [1, 2, 4, 3]. In this paper, working with coefficients in a field and starting from an AT-model (Algebraic Topological Models) of a finite regular CW-complex (see, for example, [6, 5]), an algorithm for computing some homology operations related to the elementary poset relationship between cells "to be in the boundary of" is designed at chain level. Using specialized software, an experimentation with these homology operations and others related to the cohomology algebra, applied to three-dimensional cell complexes and geometric realizations of digital volumes is done. Some interesting conclusions regarding the power of discrimination of homology operations at homotopy level and the working hypothesis of enlarging the classification of homology generators in terms of the complexity of its "boundary at homology level" are also given.

References

[1] P. Real, *On the computability of the Steenrod squares*, Annali dellÚniversita di Ferrara., **42**, Issue 1, pp.57-63 (1996)

[2] R. Gonzalez-Diaz, P. Real, *A combinatorial method for computing Steenrod squares*, J. Pure Applied Algebra, **139**, Issues 1-3, 89-108 (1999).

[3] R. Gonzalez-Diaz, P. Real, *Simplification techniques for maps in simplicial topology*, J. of Symbolic Computation, **40**, issues 4-5 pp. 1208-1224 (2005).

[4] R. Gonzalez-Diaz and P. Real,*Computation of cohomology operations on finite simplicial complexes*, Homology Homotopy Appl., **5** n.2 83Ð93, (2003).

[5] P. Pilarczyk, P. Real, *Computation of cubical homology, cohomology and (co)homological operations via chain contraction*, Adv. Comput. Math.) **41**, pp. 253-275 (2015).

[6] R. Gonzalez-Diaz, P. Real, *On the cohomology of 3D digital images*, Advances in Discrete Geometry and Topology. Discret. Appl. Math. **147** pp. 245-263 (2005).

[7] J. Kangas, S. Suuriniemi, L. Kettunen,*Algebraic structures underneath geometric approaches*, The International Journal for Computation in Mathematics in Electrical and Electronic Engineering, **30** n. 6, pp. 1715-1725 (2011).

[8] M. Desbrun, E. Kanso, Y. Tong,*Discrete Differential Forms for Computational Modeling*, Discrete Differential Geometry, Oberwolfach Seminars **38** 287-324 (2008).

[9] W.Sun, B. Starly, A. Darling, C. Gomez, *Computer-aided tissue engineering: application to biomimetic modelling and design of tissue scaffolds*,Biotechnology and Applied Biochemistry, **39**, Issue 1 49Ð58 (2004).

Nonstandard Applications of Computer Algebra

Session Organizers

Francisco Botana
Department of Applied Mathematics I
University of Vigo at Pontevedra
fbotana@uvigo.es

Antonio Hernando
Universidad Politecnica de Madrid
ahernandoe@yahoo.com

Eugenio Roanes-Lozano
Universidad Complutense de Madrid
eroanes@mat.ucm.es

Michael Wester
University of New Mexico
wester@math.unm.edu

Overview

Although all contributions to a conference have to present something new in some sense (results, algorithms, approaches, strategies, ...), this session focuses on works that while using computer algebra techniques and/or computer algebra systems, cannot be easily allocated within the usual research lines of computer algebra. Therefore, this session collects contributions that can not easily be placed in the ”standard” sessions. Examples of topics presented in previous conferences include: Verification and Development of Expert Systems (using algebraic techniques), Railway Traffic Control, Artificial Intelligence, Thermodynamics, Molecular Dynamics, Statistics, Electrical Networks, Logic, Robotics, Sociology, Integration, Mechanics, Discrete Mathematics, ...

The root lattice A_2 in the construction of tilings and algebraic hypersurfaces with many singularities

Juan García Escudero[1]

[1] *Universidad de Oviedo, Spain, jjge@uniovi.es*

In [7] we have shown that special types of simplicial arrangements of d lines contain simple arrangements which are related to a class of bivariate polynomials $J_d(x,y)$ having many critical points with few critical values. The polynomials have been used in the construction of algebraic surfaces with many A and D singularities [4, 5, 6, 7].

Tilings exhibiting non crystallographic symmetries have been significant in the past decades in the field of quasicrystals. The root lattice A_4 was considered in [1] to generate planar tilings with five-fold symmetry by projection methods. Certain pseudoline configurations inside the fundamental region of the affine Weyl group associated to the root lattice A_2 can be transformed into simple arrangements of lines containing the triangular prototiles of substitution tilings with n-fold symmetry. The analysis of the critical points of $J_d(x,y)$ allows us to define other sets of pseudolines in the fundamental region which are transformed into the simplicial arrangements containing the inflated prototiles [2]. Topological invariants of tiling spaces connected with the simplicial arrangements have been studied in ([3] and references within), where we have shown that there are five-fold and nine-fold symmetry tiling spaces having minimal first cohomology groups, a property that distinguish them from others with the same symmetries. Random tilings can be generated from both the line and the pseudoline configurations [2].

On the other hand, by following Hirzebruch's methods [9, 10] applied to special line configurations, threefolds with trivial canonical bundle and absolute value of the Euler number not large but different from zero can be obtained. Mathematica [11] and Singular [8] computer algebra systems are used.

References

[1] M. Baake, P. Kramer, M. Schlottmann and D. Zeidler, *Planar patterns with fivefold symmetry as sections of periodic structures in 4-space*, Int. J. Mod. Phys. B, **4**, pp. 2217-2268 (1990).

[2] J.G.Escudero, *Random tilings of spherical 3-manifolds*, J. Geom. Phys. **58**, pp. 1451-1464 (2008).

[3] J.G.Escudero, *Substitutions with vanishing rotationally invariant first cohomology*, Discrete Dyn. Nat. Soc. Article ID 818549, 15 p. (2012).

[4] J.G.Escudero, *Planar arrangements and singular algebraic surfaces*, in Proceedings of Applications of Computer Algebra ACA 2013, Universidad de Málaga. Spain, pp. 28-32 (2013).

[5] J.G. Escudero, *Hypersurfaces with many Aj-singularities: explicit constructions*, J. Comput. Appl. Math. **259**, pp. 87-94 (2014).

[6] J.G. Escudero, *Arrangements of real lines and surfaces with A and D singularities*, Exp. Math. **23**, pp. 482-491 (2014).

[7] J.G.Escudero, *A construction of algebraic surfaces with many real nodes*, Ann. Mat. Pura Appl, http://dx.doi.org/10.1007/s10231-015-0478-y (2015).

[8] G.M. Greuel and G. Pfister, *A Singular introduction to commutative algebra*, Springer (2008).

[9] F. Hirzebruch, *Some examples of algebraic surfaces,* in Proceedings 21st Summer Research Institute Australian Mathematical Society. Contemporary Mathematics **9**, pp. 55-71, Amer.Math.Soc. (1982).

[10] F. Hirzebruch, *Some examples of threefolds with trivial canonical bundle*, in Gesammelte Abhandlungen, Bd. II, pp. 757-770, Springer (1987).

[11] S.Wolfram, *Mathematica*, Addison-Wesley Publishing Co. (1991).

Computer Algebra-based RBES personalized menu generator

E. Roanes-Lozano[1], J.L. Galán-García[2], G. Aguilera-Venegas[2]

[1] *Instituto de Matemática Interdisciplinar (IMI) & Algebra Dept., Universidad Complutense de Madrid, Spain, eroanes@mat.ucm.es*
[2] *Applied Mathematics Dept., Universidad de Málaga, Spain, jl_galan@uma.es,gabri@ctima.uma.es*

People have many constraints concerning the food they eat. These constraints can be based on religious believes, be due to food allergies or to illnesses, or can be derived just from personal preferences. Therefore, preparing menus at hospitals and restaurants can be really complex. Another special situation arise when traveling abroad. It is not always enough to know the brief description in the restaurant menu or the explanation of the waiter. For example, “calamares en su tinta” (squid in its own ink) is a delicious typical Spanish dish, not well-known abroad. Its brief description would be “squid with boiled rice in its own (black) ink”. But an ingredient (included in a small amount, in order to thicken the sauce) is flour, a fact very important for someone suffering from celiac disease. Therefore, we have considered that it would be very interesting to develop a Rule Based Expert System (RBES) to address these problems. The rules derive directly from the recipes and contain the information about required ingredients and names of the dishes. We distinguish: ingredients and ways of cooking, intermediate products (like “mayonnaise”, that doesn’t always appear explicitly in the restaurants’ menus) and final products (like “seafood cocktail”, that are the dishes listed in the restaurant menu). For each customer at a certain moment, the input to the system are: on one hand, the stock of ingredients at that moment, and on the other, the religion, allergies and restrictions due to illnesses or personal preferences of the customer. The RBES then constructs a “personalized restaurant menu” using set operations and knowledge extraction (thanks to an algebraic Groebner bases-based inference engine[1]). The RBES has been implemented in the computer algebra system *Maple^{TM}18* (using its convenient *Embedded Components*) and can be run from computers and tablets using *Maple^{TM}* or the *Maple^{TM}Player*.

References

[1] E. Roanes-Lozano, L.M. Laita, A. Hernando and E. Roanes-Macías, *An Algebraic Approach to Rule Based Expert Systems*, RACSAM Rev. R. Acad. Cien. Serie A. Mat. **104**, 1, pp 19-40 (2010). DOI: 10.5052/RACSAM.2010.04

Symbolic-Numeric Computing: A Polynomial System Arising in Image Analysis of Point Cloud Data

Robert H. Lewis[1]

[1] *Fordham University, New York, NY 10458, USA, rlewis@fordham.edu*

Systems of polynomial equations with parameters arise in many fields, such as geometric computing, flexibility of molecules, chemical reactions, game theory, image analysis, operations research, and differential equations. In most applied problems, the best method for their symbolic solution is the Dixon-EDF resultant [**?**]. We will briefly describe the method itself, then discuss a problem arising from surface reconstruction from point cloud data. We focus on our recent work with B. Palancz and J. Awange on image analysis. Given a point cloud created by a laser scan (LIDAR) [**?**], we want to discern underlying shapes. This entails separating “inliers" from “outliers" by the maximization of the likelihood function of a dual Gaussian mixture distribution. This is fine example of a symbolic-numeric method.

We introduce a new robust technique employing expectation maximization to separate outliers (extraneous data points) from inliers (true data points) iteratively, represented by different Gaussian distributions. Since in every iteration step, a new parameter estimation should be carried out, a key point is to solve this parameter estimation as fast as possible. To do that, the problem of numerical global maximization of the likelihood function of the Gaussian mixture was transformed into the solution of a multivariate polynomial system. The symbolic solution of the resulting polynomial system consisting of four equations is quite challenging because of the high number of parameters. In order to solve it, a linear transformation was required to reduce the total degrees of the polynomials. This reduced system was solved successfully via Dixon-EDF resultant method.

Some of this was reported on at ACA 2014 [**?**]. However, there is now a significant new numerical technique used in the iterative step. We compare our results with other robust methods such as Danish and Random Sample Consensus methods on the data set of a real laser scanning experiment. We find that our method is much faster and more robust.

References

[1] Huang C-M and Tseng Y-H. *Plane fitting methods of Lidar point cloud*, Dept. of Geomatics, National Cheng Kung Uni. Taiwan (2008)

[2] R. H. Lewis. *Heuristics to Accelerate the Dixon Resultant*, Mathematics and Computers in Simulation **77**, 4, pp. 400 - 407, (2008)

[3] R. H. Lewis, Palancz B and Awange JL *Application of Dixon resultant to maximization of the likelihood function of Gaussian mixture distribution*. ACA Conference, New York, USA (2014)

Making more flexible ATISMART+ model for traffic simulations using a CAS

M. Ramírez, J.M. Gavilán, G. Aguilera, J.L. Galán, M.Á. Galán, P. Rodríguez

University of Málaga, Spain, jlgalan@uma.es

Traffic simulations usually require the search of a path to join two different points. Dijkstra's algorithm [1] is one of the most commonly used for this task due to its easiness and quickness. In [2, 3] we developed an accelerated time simulation of car traffic in a smart city using Dijkstra's algorithm to compute the paths.

Dijkstra's algorithm provides a shortest path between two different points but this is not a realistic situation for simulations. For example, in a car traffic situation, the driver may not know the shortest path to follow. This ignorance can be produced, among others, because one of the following two facts: the driver may not know the exact length of the lanes, or, even knowing the exact length, the driver may not know how to find the shortest path. Even more, in many cases, a mixture of both facts occurs.

A more realistic simulation should therefore consider these kind of facts. The algorithm used to compute the path from one point to another in a traffic simulation might consider the possibility of not using the shortest path.

In this talk, we use a new probabilistic extension of Dijkstra's algorithm which covers the above two situations. For this matter, two different modifications in Dijkstra's algorithm have been introduced: using non-exact length in lanes, and the choice of a non-shortest path between two different points. Both modifications are used in a non-deterministic way by means of using probability distributions (classical distributions such as Normal or Poisson distributions or even "ad hoc" ones). A precise, fast, natural and elegant way of working with such probability distributions is the use of a CAS in order to deal with exact and explicit computations.

As an example of use of this extension of Dijkstra's algorithm, we will show the ATISMART+ model. This model provides more realistic accelerated time simulations of car traffics in a smart city and was first introduced in [4] and extended in [5]. This model was developed combining JAVA for the GUI and MAXIMA for the mathematical core of the algorithm.

The studies developed in the above mentioned works, dealt with Poisson, Exponential, Uniform and Normal distributions. In this talk we will introduce, as a novelty, the possibility of using other continuous probability distributions such as: Lognormal, Weibul, Gamma, Beta, Chi-Square, Student's t, Z, Pareto, Logistic, Cauchy or Irwin-Hall, and other discrete distributions such as: Bernouille, Rademacher, Binomial, Geometric, Negative Binomial or Hypergeometric. Even more, this new version allows to deal with any “ad-hoc” continuous, discrete or mixed user’s distributions. This fact improves the flexibility of ATISMART+ model.

References

[1] E. W. Dijkstra. A note on two problems in connexion with graphs. Numerische Mathematik 1 (1959) 269–271.

[2] José Luis Galán, Gabriel Aguilera, José Carlos Campos, Pedro Rodríguez. Simulating Car Traffic with Smart Signals using a CAS (Abstract). In J. L. Galán–García, G. Aguilera–Venegas, Pedro Rodríguez–Cielos (eds.): Aplications of Computer Algebra ACA’2013 Proceedings. Málaga, 2013, pp. 183.

[3] José L. Galán-García, Gabriel Aguilera-Venegas and Pedro Rodríguez-Cielos. An Accelerated-Time Simulation for Traffic Flow in a Smart City. J. Comput. and Appl. Math. 270 (2014) 557–563.

[4] José Luis Galán-García, Gabriel Aguilera-Venegas, María Á. Galán-García, Pedro Rodríguez. Simulating Realistic Traffic Flow in a Smart City (Abstract). In Proceedings of the 4th European Seminar on Computing ESCO 2014. Pilsen, Czech Republic, 2014, pp. 29.

[5] José L. Galán-García, Gabriel Aguilera-Venegas, María Á. Galán-García and Pedro Rodríguez-Cielos. A new Probabilistic Extension of Dijkstra’s Algorithm to simulate more realistic traffic flow in a smart city. J. Applied Mathematics and Computation. In press. Doi: 10.1016/j.amc.2014.11.076.

Properties of the Simson–Wallace locus applied on a skew quadrilateral

P. Pech[1]

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

The well-known Simson–Wallace theorem reads [3]:

Let K, L, M be orthogonal projections of a point P onto the sides of a triangle ABC. Then the locus of P such that K, L, M are collinear, is the circumcircle of ABC.

This theorem has several generalizations [4], [5], [10],[6], [7], [9]. A generalization of the Simson–Wallace theorem which is by [2] ascribed to J. D. Gergonne is as follows:

Let K, L, M be orthogonal projections of a point P onto the sides of a triangle ABC. Then the locus of P such that the area of the triangle KLM is constant, is the circle through P which is concentric with the circumcircle of ABC.

If we consider a tetrahedron $ABCD$ instead of a triangle ABC then we can investigate the locus of points $P \in E^3$ whose orthogonal projections onto the faces of $ABCD$ are coplanar or form a tetrahedron of a constant volume. This was studied in [10], [6], [7], [9].

The generalization of Simson–Wallace theorem on *skew quadrilaterals* in the Euclidean 3D space is as follows [6], [8]:

The locus of a point P whose orthogonal projections K, L, M, N onto the sides on a skew quadrilateral $ABCD$ form a tetrahedron of a constant volume s is a cubic surface G.

By searching for the locus and its properties we applied computer aided coordinate method based on Groebner bases computation and Wu–Ritt method using the software CoCoA [1] and the Epsilon library [11] working under Maple.

The cubic surface G can be investigated from various points of view. In [8] reducibility of G with $s = 0$ was explored. The following conjecture was stated: The Simson–Wallace locus which is a cubic surface G is decomposable iff two pairs of sides a skew quadrilateral $ABCD$ are of equal lengths. If for instance $|AB| = |BC| = a$ and $|CD| = |DA| = b$, then in the case $a \neq b$ the cubic G decomposes into a plane and a one-sheet hyperboloid, and if $a = b$ we get three mutually orthogonal planes.

In the talk further properties of G are studied. It is well known that the maximum number of lines of a general cubic surface is 27. There is a question how many lines do lie on the cubic G? It seems that the maximum number of lines lying on G is 15. This issue is also connected with the number of the so called tritangent planes which intersect the cubic surface in three lines. Knowing these planes enables us to express G in the form of sum of two cubics which resolve into the product of three linear factors which describe the tritangent planes.

References

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

[2] Chou, S. C.: *Mechanical Geometry Theorem Proving*. D. Reidel Publishing Company, Dordrecht (1987).

[3] Coxeter, H. S. M., Greitzer, S. L: *Geometry revisited*, Toronto New York (1967).

[4] Giering, O.: *Affine and Projective Generalization of Wallace Lines*, J. Geometry and Graphics **1**, 119-133 (1997).

[5] Guzmán, M:*An Extension of the Wallace–Simson Theorem: Projecting in Arbitrary Directions*, Amer. Math. Monthly **106**, 574-580 (1999).

[6] Pech, P.: *On Simson–Wallace Theorem and Its Generalizations*, J. Geometry and Graphics **9**, 141-153 (2005).

[7] Pech, P.: *On a 3D extension of the Simson–Wallace theorem*, J. Geometry and Graphics, **18**, 205-215 (2014).

[8] P. Pech: *Extension of Simson–Wallace theorem on skew quadrilaterals and further properties*, in *Lecture Notes in Artificial Intelligence* (ADG-2014), Springer 2015, to appear.

[9] Riesinger, R.: *On Wallace Loci from the Projective Point of View*, J. Geometry and Graphics **8**, 201-213 (2004).

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

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

Properties of the Simson–Wallace locus applied on a skew quadrilateral

P. Pech[1]

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

The well-known Simson–Wallace theorem reads [3]:

Let K, L, M be orthogonal projections of a point P onto the sides of a triangle ABC. Then the locus of P such that K, L, M are collinear, is the circumcircle of ABC.

This theorem has several generalizations [4], [5], [10],[6], [7], [9]. A generalization of the Simson–Wallace theorem which is by [2] ascribed to J. D. Gergonne is as follows:

Let K, L, M be orthogonal projections of a point P onto the sides of a triangle ABC. Then the locus of P such that the area of the triangle KLM is constant, is the circle through P which is concentric with the circumcircle of ABC.

If we consider a tetrahedron $ABCD$ instead of a triangle ABC then we can investigate the locus of points $P \in E^3$ whose orthogonal projections onto the faces of $ABCD$ are coplanar or form a tetrahedron of a constant volume. This was studied in [10], [6], [7], [9].

The generalization of Simson–Wallace theorem on *skew quadrilaterals* in the Euclidean 3D space is as follows [6], [8]:

The locus of a point P whose orthogonal projections K, L, M, N onto the sides on a skew quadrilateral $ABCD$ form a tetrahedron of a constant volume s is a cubic surface G.

By searching for the locus and its properties we applied computer aided coordinate method based on Groebner bases computation and Wu–Ritt method using the software CoCoA [1] and the Epsilon library [11] working under Maple.

The cubic surface G can be investigated from various points of view. In [8] reducibility of G with $s = 0$ was explored. The following conjecture was stated: The Simson–Wallace locus which is a cubic surface G is decomposable iff two pairs of sides a skew quadrilateral $ABCD$ are of equal lengths. If for instance $|AB| = |BC| = a$ and $|CD| = |DA| = b$, then in the case $a \neq b$ the cubic G decomposes into a plane and a one-sheet hyperboloid, and if $a = b$ we get three mutually orthogonal planes.

In the talk further properties of G are studied. It is well known that the maximum number of lines of a general cubic surface is 27. There is a question how many lines do lie on the cubic G? It seems that the maximum number of lines lying on G is 15. This issue is also connected with the number of the so called tritangent planes which intersect the cubic surface in three lines. Knowing these planes enables us to express G in the form of sum of two cubics which resolve into the product of three linear factors which describe the tritangent planes.

References

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

[2] Chou, S. C.: *Mechanical Geometry Theorem Proving*. D. Reidel Publishing Company, Dordrecht (1987).

[3] Coxeter, H. S. M., Greitzer, S. L: *Geometry revisited*, Toronto New York (1967).

[4] Giering, O.: *Affine and Projective Generalization of Wallace Lines*, J. Geometry and Graphics **1**, 119-133 (1997).

[5] Guzmán, M:*An Extension of the Wallace–Simson Theorem: Projecting in Arbitrary Directions*, Amer. Math. Monthly **106**, 574-580 (1999).

[6] Pech, P.: *On Simson–Wallace Theorem and Its Generalizations*, J. Geometry and Graphics **9**, 141-153 (2005).

[7] Pech, P.: *On a 3D extension of the Simson–Wallace theorem*, J. Geometry and Graphics, **18**, 205-215 (2014).

[8] P. Pech: *Extension of Simson–Wallace theorem on skew quadrilaterals and further properties*, in *Lecture Notes in Artificial Intelligence* (ADG-2014), Springer 2015, to appear.

[9] Riesinger, R.: *On Wallace Loci from the Projective Point of View*, J. Geometry and Graphics **8**, 201-213 (2004).

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

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

Polynomial System Solving, Gröbner Basis, and Applications

Session Organizers

Christian Eder
University of Kaiserslautern
ederc@mathematik.uni-kl.de

Jean-Charles Faugère
UPMC, INRIA PolSys Team, Paris
Jean-Charles.Faugere@inria.fr

Ludovic Perret
LIP6-UPMC/CNRS/Inria, Paris
ludovic.perret@lip6.fr

Elias Tsigaridas
UPMC, INRIA PolSys Team, Paris
Elias.Tsigaridas@inria.fr

Overview

Polynomial systems are fundamental mathematical objects and emanate naturally in almost the whole spectrum of science. They arise in computational geometry, optimization, tensor decomposition, game theory, coding theory, cryptology, CAD, signal processing, robotics, biology; just to mention few of the disciplines.

Groebner bases, on the other hand, are one of the main tools for solving systems of polynomial equations. Moreover, they are the building blocks for a wide range of higher-level computer algebra algorithms.

The special session focuses on algorithms, efficient implementations for solving polynomial systems and on novel applications that extend the limits of the state-of-the-art from a theoretical and/or practical point of view. Its purpose is to bring together different communities that are interested in polynomial system solving, to present cutting-edge results in the area and to identify future challenges.

Improved Parallel Gaussian Elimination for Gröbner Bases Computations in Finite Fields

B. Boyer[1], C. Eder[2], J.-C. Faugère[3], S. Lachartre[4], F. Martani[5]

[1] INRIA, *Équipe* POLSYS, *Centre Paris – Rocquencourt*
Sorbonne Universite, UPMC *Paris 6, Équipe* POLSYS. LIP6
CNRS, UMR-*7606,* LIP6
F-75005, Paris, France
brice.boyer@lip6.fr
[2] *University of Kaiserslautern*
Department of Mathematics
PO Box 3049
67653 Kaiserslautern, Germany
ederc@mathematik.uni-kl.de
[3] INRIA, *Équipe* POLSYS, *Centre Paris – Rocquencourt*
Sorbonne Universite, UPMC *Paris 6, Équipe* POLSYS. LIP6
CNRS, UMR-*7606,* LIP6
F-75005, Paris, France
jean-charles.faugere@inria.fr
[4] *Thalès Group*
sylvian.lachartre@thalesgroup.com
[5] *martani.net@gmail.com*

We present a GPLv2 open source C library for linear algebra specialized for eliminating matrices generated during Gröbner basis computations in algorithms like F4 or F5. We improve on the initial ideas of Faugère and Lachartre (FL reduction). Our approach takes even more advantage of the very special structure the corresponding matrices have: quasi unit-triangular sparse matrices with patterns in the data. Optimizing this reduction step is crucial for the overall Gröbner basis computation.

We first present improved data structures for storing these FL matrices in binary format, namely by compressing the repeated data in the rows and the column indexes, before gzip-ing the result. We can save up to an order of magnitude in space, allowing us to produce and share a large database of such matrices for benchmarking and testing purpose. We show efficient blocked data structures for computing the reduced forms with specialized AXPY and TRSM operations, that take advantage of the patterns in the matrices and their sparsity. For instance, a special *multiline* storage allows cache friendly storage of sparse rows. We also reduce the number of operations, in a parallel friendly fashion, by changing the order of the operations in the elimination and by not computing the full row echelon form. Finally, we present experimental results for sequential and parallel computations on NUMA architectures. With our new implementation we get a 5-10% speed-up for the se-

quential algorithm depending on the rank. We also get better scaling up until 32 (non hyper-threaded) cores instead of 16: we have speed-ups around 14 or 16 for bigger benchmarks. We also save more than twice the amount of memory used during the computation.

References

[1] B. Boyer, J.-G. Dumas, P. Giorgi, C. Pernet, and B. Saunders. Elements of design for containers and solutions in the linbox library. In H. Hong and C. Yap, editors, *Mathematical Software – ICMS 2014*, volume 8592 of *Lecture Notes in Computer Science*, pages 654–662. Springer Berlin Heidelberg, 2014.

[2] L. Dagum and R. Menon. Openmp: an industry standard api for shared-memory programming. *Computational Science & Engineering, IEEE*, 5(1):46–55, 1998.

[3] J. Dumas, T. Gautier, C. Pernet, and Z. Sultan. Parallel computation of echelon forms. In F. M. A. Silva, I. de Castro Dutra, and V. S. Costa, editors, *Euro-Par 2014 Parallel Processing - 20th International Conference, Porto, Portugal, August 25-29, 2014. Proceedings*, volume 8632 of *Lecture Notes in Computer Science*, pages 499–510. Springer, 2014.

[4] J.-G. Dumas, T. Gautier, M. Giesbrecht, P. Giorgi, B. Hovinen, E. L. Kaltofen, B. D. Saunders, W. J. Turner, and G. Villard. LinBox: A generic library for exact linear algebra. In *Proceedings of the 2002 International Congress of Mathematical Software, Beijing, China*. World Scientific Pub, Aug. 2002.

[5] J.-G. Dumas, P. Giorgi, and C. Pernet. Dense linear algebra over word-size prime fields: the FFLAS and FFPACK packages. *ACM Trans. Math. Softw.*, 35(3):1–42, 2008.

[6] J.-G. Dumas and G. Villard. Computing the rank of sparse matrices over finite fields. In V. G. Ganzha, E. W. Mayr, and E. V. Vorozhtsov, editors, *CASC'2002, Proceedings of the fifth International Workshop on Computer Algebra in Scientific Computing, Yalta, Ukraine*, pages 47–62. Technische Universität München, Germany, September 2002.

[7] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1–3):61–88, June 1999.

[8] J.-C. Faugère and S. Lachartre. Parallel Gaussian Elimination for Gröbner bases computations in finite fields. In M. Moreno-Maza and J. L. Roch, editors, *Proceedings of the 4th International Workshop on Parallel and Symbolic Computation*, PASCO '10, pages 89–97, New York, NY, USA, July 2010. ACM.

[9] J.-C. Faugère and S. Lachartre. Parallel Gaussian Elimination for Gröbner bases computations in finite fields. In M. Moreno-Maza and J. L. Roch, editors, *Proceedings of the 4th International Workshop on Parallel and Symbolic Computation*, PASCO '10, pages 89–97, New York, NY, USA, July 2010. ACM.

[10] T. Gautier, X. Besseron, and L. Pigeon. Kaapi: A thread scheduling runtime system for data flow computations on cluster of multi-processors. In *Proceedings of the 2007 International Workshop on Parallel Symbolic Computation*, PASCO '07, pages 15–23, New York, NY, USA, 2007. ACM.

[11] S. Lachartre. *Algèbre linéaire dans la résolution de systèmes polynomiaux Applications en cryptologie*. PhD thesis, Université Paris 6, 2008.

Sparse multihomogeneous systems: root counts and discriminants

Ioannis Z. Emiris

U. Athens, Greece

Motivated by sparse multilinear systems expressing Nash equilibria, we study sparse semimixed multihomogeneous systems. The theory to exploit sparseness is toric elimination and Newton polytopes. In the case of Nash equilibria, polynomials are multilinear but do *not* contain all possible terms. The term “semimixed” implies that complexity bounds depend on the number of distinct Newton polytopes of the given system.

We derive a generating function for the mixed volume of a family of systems expressing Nash equilibria. In the more general case, where every Newton polytope is the Minkowski sum of scaled copies of a fixed set of polytopes, we write the mixed volume in terms of these polytope volumes and the permanent of the scaling factors. These results were presented in [EV14].

Determinantal formulae are fundamental in computing with resultants, but have not been obtained for discriminants in nontrivial cases. In a more recent work, and back to Nash equilibria, we derive a determinantal formula for the discriminant of the corresponding well constrained system.

This is joint work with Raimundas Vidunas (now with U. Tokyo).

References

[EV14] I.Z. Emiris and R. Vidunas. Root counts of semi-mixed systems, and an application to counting Nash equilibria. In *Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation*, pages 154–161, Kobe, Japan, 2014. ACM Press.

Tropical Homotopy Continuation

Anders Jensen
Department of Mathematics,
Aarhus University

In numerical algebraic geometry the key idea is to solve systems of polynomial equations via homotopy continuation. By this is meant, that the solutions of a system are tracked as the coefficients change continuously toward the system of interest. We study the tropicalisation of this process. Namely, we combinatorially keep track of the solutions of a tropical polynomial system as its coefficients change. Tropicalising the entire regeneration process of numerical algebraic geometry, we obtain a combinatorial algorithm for finding all tropical solutions. In particular, we obtain the mixed cells of the system. Experiments suggest that the method is not only competitive, but also asymptotically performs better than conventional methods for mixed cell enumeration. It currently does not perform as well as a recent method by Malajovich. However, using symbolic perturbations, reverse search and exact arithmetic our method becomes reliable, memory-less and well-suited for parallelisation.

Bounds on the Number of Real Solutions For a Family of Fewnomial Systems of Equations via Gale Duality

Daniel J. Bates[1], Jonathan D. Hauenstein[2], Matthew Niemerg[3], Frank Sottile[4]

[1] *Colorado State University, Fort Collins, CO bates@math.colostate.edu*
[2] *Notre Dame University, South Bend, IN hauenstein@nd.edu*
[3] *Fields Institute, Toronto, Canada research@matthewniemerg.com*
[4] *Texas A&M University sottile@math.tamu.edu*

We give a Descartes'-like bound on the number of positive solutions to a system of fewnomials that holds when its exponent vectors are not in convex position and a sign condition is satisfied. This was discovered while developing algorithms and software for computing the Gale transform of a fewnomial system.

Linear Algebra for Computing Gröbner Bases of Linear Recursive Multidimensional Sequences

J. Berthomieu, B. Boyer, **J.-C. Faugère**

Sorbonne Universités, UPMC Univ Paris 06, Équipe PolSys, LIP6

CNRS UMR 7606, LIP6

INRIA, Équipe PolSys, Centre Paris – Rocquencourt

jeremy.berthomieu@lip6.fr,
jean-charles.faugere@inria.fr,
brice.boyer@lip6.fr

Sakata generalized the Berlekamp – Massey algorithm to n dimensions in 1988. The Berlekamp – Massey – Sakata (BMS) algorithm can be used for finding a Gröbner basis of a 0-dimensional ideal of relations verified by a table. We investigate this problem using linear algebra techniques, with motivations such as accelerating change of basis algorithms (FGLM) or improving their complexity. We first define and characterize multidimensional linear recursive sequences for 0-dimensional ideals. Under genericity assumptions, we propose a randomized preprocessing of the table that corresponds to performing a linear change of coordinates on the polynomials associated with the linear recurrences. This technique then essentially reduces our problem to using the efficient 1-dimensional Berlekamp – Massey (BM) algorithm. However, the number of probes to the table in this scheme may be elevated. We thus consider the table in the black-box model: we assume probing the table is expensive and we minimize the number of probes to the table in our complexity model. We produce an FGLM-like algorithm for finding the relations in the table, which lets us use linear algebra techniques. Under some additional assumptions, we make this algorithm adaptive and reduce further the number of table probes. This number can be estimated by counting the number of distinct elements in a multi-Hankel matrix (a multivariate generalization of Hankel matrices); we can relate this quantity with the geometry of the final staircase. Hence, in favorable cases such as convex ones, the

complexity is essentially linear in the size of the output. Finally, when using the LEX ordering, we can also make use of fast structured linear algebra similarly to the Hankel interpretation of Berlekamp – Massey.

Nearly optimal algorithms for real and complex root refinement

Elias Tsigaridas
INRIA, Équipe PolSys, Centre Paris – Rocquencourt
Sorbonne Universités, UPMC Univ Paris 06, Équipe PolSys, LIP6
CNRS UMR 7606, LIP6
elias.tsigaridas@inria.fr

We combine some powerful techniques developed in the area of univariate root finding to devise new algorithms for refinement of isolated complex and real roots that have nearly optimal Boolean complexity. One of the main ingredients is multipoint evaluation, which in turn is closely related to fast computations with structured matrices.

Joint work with Victor Pan (CUNY, USA).

A Fast Euclid-type Algorithm for Quasiseparable Polynomials

Sirani M. Perera[1]

[1] *Daytona State College, Daytona Beach, USA, pereras@daytonastate.edu*

In [3], a Schur-type algorithm was presented to compute a recursive triangular factorization $R = LU$ for a strongly non-singular $n \times n$ matrix R satisfying the displacement equation:

$$RY - VR = GH^T$$

with upper and lower Hessenberg matrices Y and V respectively, and $n \times \alpha$ matrices G and H where α is small comparing with n. The classification paper [1] generalized quasiseparable polynomials $Q_k(x)(k = 1,2,\cdots,n-1)$ satisfying the EGO-type [2] recurrence relation:

$$\begin{bmatrix} G_k(x) \\ Q_k(x) \end{bmatrix} = \begin{bmatrix} \alpha_k & \beta_k \\ \gamma_k & \delta_k x + \theta_k \end{bmatrix} \begin{bmatrix} G_{k-1}(x) \\ Q_{k-1}(x) \end{bmatrix} \tag{1}$$

where $G_k(x)$ are auxiliary polynomials. These quasiseparable polynomials are categorized as the super class of the orthogonal polynomials $Q_k(x)$ (orthogonal with respect to weighted inner product (definite or indefinite) on the real line) satisfying the three term recurrence relation:

$$Q_k(x) = (\alpha_k x - \delta_k)Q_{k-1}(x) - \gamma_k \cdot Q_{k-2}(x), \qquad (k = 1,2,\cdots,n-1)$$

and also the super class of the Szegö polynomials $\phi_k^\sharp(x)(k = 1,2,\cdots,n-1)$ (orthogonal on the unit circle with respect to weighted inner product) satisfying two-term recurrence relations:

$$\begin{bmatrix} \phi_k(x) \\ \phi_k^\sharp(x) \end{bmatrix} = \frac{1}{\mu_0}\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad \begin{bmatrix} \phi_k(x) \\ \phi_k^\sharp(x) \end{bmatrix} = \frac{1}{\mu_k}\begin{bmatrix} 1 & -\rho_k^\sharp \\ -\rho_k & 1 \end{bmatrix}\begin{bmatrix} \phi_{k-1}(x) \\ x\phi_{k-1}^\sharp(x) \end{bmatrix}$$

where ρ_k are reflection coefficients and μ_k are complementary parameters.

In this talk, we first address $O(n^2)$ Euclid-type algorithm as a Schur algorithm for the matrices with displacement structure

$$C_a^T S - SC_a = 0 \tag{2}$$

where S is the Bezoutian matrix associated to the reverse polynomials: $a^\sharp(x) = a_n + a_{n-1}x + \cdots + a_0x^n$ and $b^\sharp(x) = b_n + b_{n-1}x + \cdots + b_0x^n$ and C_a is the companion matrix associated to the polynomial $a(x) = a_0 + a_1 x + \cdots + a_n x^n$. The displacement equation (2) is a variant of $Lancaster - Tismenetsky$ equation in [4].

Later on, we address more generalized $O(n^2)$ Euclid-type algorithms for the wider class of polynomials which we call quasiseparable polynomials satisfying recurrence relations (1), by generalizing the displacement equation (2) via Bezoutian matrix S for the quasiseparable polynomials and companion matrix C_a to the confederate matrix.

References

[1] T. Bella, V. Olshevsky, and P. Zhlobich, *Classifications of recurrence relations via subclasses of (H,k)-quasiseparable matrices*, Numerical Linear Algebra in Signals, Systems and Control, Springer-Verlag, Lecture Notes in Electrical Engineering, **80, 1** (2011), 23-54.

[2] Y. Eidelman, I. Gohberg and V. Olshevsky, *Eigenstructure of Order-One-Quasiseparabale Matrices. Three-term and Two-term Recurrence Relations*, Linear algebra and its applications, **405** (2005), 1-40.

[3] G. Heinig and V. Olshevsky, *The Schur algorithm for matrices with Hessenberg displacement structure*, Structured Matrices in Mathematics, Computer Science, and Engineering II, Contemporary Mathematics series, **281** (2001), 3-16.

[4] P. Lancaster and M. Tismenetsky, *The Theory of Matrices, Second Edition: With Applications (Computer Science and Scientific Computing)*, Academic Press, 2 edition, 1985.

Midway upon the journey

John Perry
Department of Mathematics
The University of Southern Mississippi

Unlike traditional, *static* algorithms to compute a Gröbner basis, a *dynamic* algorithm does not require a term ordering as input, but tries to compute an efficient term ordering as the computation proceeds, returning both a final ordering, and a Gröbner basis with respect to that ordering. Caboara first implemented the dynamic algorithm twenty years ago, and for the next two decades that was also the last published implementation.

Last year, we reported on a new, study implementation of a new dynamic algorithm, which adopts ideas from polyhedral geometry to greatly improve performance, especially for dense polynomial systems. That implementation used semi-compiled Python in Sage, so it was impossible to make comparisons on the practical speed of the newer algorithm. Since then, we have re-implemented it in Singular using C++, using the same procedures and data structures as Singular's `std()` algorithm, giving a firm basis for serious comparisons with a traditional algorithm.

A dynamic algorithm naturally requires a means of deciding which ordering is preferable. We compare the traditional, Hilbert heuristic to several others, some of our own devising, and some suggested by others, and conclude with some remarks on the next major phase of our project, a signature-based dynamic algorithm.

Application of Computer Algebra in Number Theory Based Cryptology

Guénaël Renault[1]

[1] *Université Pierre et Marie Curie, INRIA, CNRS, LIP6, Paris, France*

In Eurocrypt'14 [1], we presented results on the use of torsion points for increasing the efficiency of index calculus algorithm for solving the DLP in an elliptic curve E of characteristic 2. To obtain these results, we mainly use the underlying symmetries of the problem of finding the roots of a given multivariate polynomials. These polynomials, called Semaev's summation polynomials, encode the problem of decomposing a given point in E as a sum of m elements in a factor base. Their size increases exponentially in m^2 and thus the computation of summation polynomials is challenging. The largest ones computed so far correspond to $m = 5$. In this talk, I will focus on the method, mainly based on computer algebra tools, we developed for computing summation polynomials for $m = 7$ in the case of characteristic 2, which represents a new record.

References

[1] Jean-Charles Faugère, Louise Huot, Antoine Joux, Guénaël Renault, Vanessa Vitse. *Symmetrized Summation Polynomials: Using Small Order Torsion Points to Speed Up Elliptic Curve Index Calculus*, Advances in Cryptology EUROCRYPT 2014, Springer, LNCS, Vol. 8441, pp 40-57.

The HIMMO Scheme

Ludo Tolhuizen
Philips Group Innovation, Research, Eindhoven, The Netherlands

The recently introduced HIMMO scheme enables lightweight identity-based key sharing and verification of credentials in a non-interactive way. The collusion resistance properties of HIMMO enable direct secure communication between any pair of Internet-connected devices. The facts that attacking HIMMO requires lattice techniques and that it is extremely lightweight make HIMMO an ideal lightweight approach for key agreement and information verification in a post-quantum world. In this presentation we explain the HIMMO scheme, that is based on polynomial evaluations, address its applications and discuss two lattice-based attacks.

Algebraic Attack against Variants of McEliece with Goppa Polynomial of a Special Form

Jean-Charles Faugère[1,2,3], Ludovic Perret[2,1,3], and
Frédéric de Portzamparc[4,1,2,3]

INRIA, Paris-Rocquencourt Center[1],
UPMC Univ Paris 06, UMR 7606, LIP6, F-75005, Paris, France[2]
CNRS, UMR 7606, LIP6, F-75005, Paris, France[3]
Gemalto, 6 rue de la Verrerie 92190, Meudon, France[4]
`jean-charles.faugere@inria.fr, ludovic.perret@lip6.fr,`
`frederic.urvoydeportzamparc@gemalto.com`

Abstract. In this talk, we present a new algebraic attack against some special cases of Wild McEliece Incognito, a generalization of the original McEliece cryptosystem. This attack does not threaten the original McEliece cryptosystem. We prove that recovering the secret key for such schemes is equivalent to solving a system of polynomial equations whose solutions have the structure of a usual *vector space*. Consequently, to recover a basis of this vector space, we can greatly reduce the number of variables in the corresponding algebraic system. From these solutions, we can then deduce the basis of a GRS code. Finally, the last step of the cryptanalysis of those schemes corresponds to attacking a McEliece scheme instantiated with particular GRS codes (with a polynomial relation between the support and the multipliers) which can be done in polynomial-time thanks to a variant of the Sidelnikov-Shestakov attack. For Wild McEliece & Incognito, we also show that solving the corresponding algebraic system is notably easier in the case of a non-prime base field $\mathbb{F}_q$. To support our theoretical results, we have been able to practically break several parameters defined over a non-prime base field $q \in \{9, 16, 25, 27, 32\}$, $t \leq 6$, extension degrees $m \in \{2, 3\}$, security level up to 2^{129} against information set decoding in few minutes or hours.

Keywords. public-key cryptography, McEliece cryptosystem, algebraic cryptanalysis.

Use of Gröbner basis in order to perform a fault attack in pairing-based cryptography

Nadia El Mrabet[1], E. Fouotsa[2],

[1] *LIASD - University Paris 8 and SAS - CGCP EMSE Gardanne, {nadia.el-mrabet}@emse.fr*
[2] *LMNO, University of Caen, emmanuel.fouotsa@unicaen.fr*

Pairings are mathematical tools that have been proven to be very useful in the construction of many cryptographic protocols. Some of these protocols are suitable for implementation on power constrained devices such as smart cards or smartphone which are subject to side channel attacks.

In this paper, we analyse the efficiency of the point blinding countermeasure in pairing based cryptography against side channel attacks. In particular,we show that this countermeasure does not protect Miller's algorithm for pairing computation against fault attack. We then give recommendation for a secure implementation of a pairing based protocol using the Miller algorithm.

Pairings are bilinear maps defined on the group of rationals points of elliptic or hyper elliptic curves. Several protocols using pairings were proposed in the literature [5]. Among these protocols, only those constructed on the identity based model involve a secret which is one of the argument during the computation of a pairing. The implementation of a pairing based protocol is efficient enough to allow the use of pairing based cryptography on power constrained device such as smart cards and mobile phones [4]. Smart cards are by nature sensitive to side channel attacks. Side channel attacks are powerful attacks that use the implementation of a protocol to obtain information on the secret. They are divided into two families: invasive and non invasive attacks. Invasive attacks are based on the model of fault attacks. The execution of a protocol is disturbed, the result is then a faulty one and the analysis of this faulty result can provide information on the secret. In non invasive attacks, the information can be leaked by the time of execution, the electric consumption or the electromagnetic emission of the device. Several works have investigated the robustness of identity based cryptography to side channel attacks. They are mainly focused on fault attacks [6, 1]. As the secret during an identity based protocol can be recovered by side channel attacks, several countermeasures were proposed. Those countermeasures are the same for invasive and non invasive attacks [3].

In [2] we analyze the efficiency of the point blinding countermeasure in pairing based cryptography. As the most efficient pairings are constructed on the model of the Tate pairing, we focus on the Miller algorithm, used for the Tate pairing considering Weierstrass elliptic curve. Obviously, this analysis is the same for the (optimal) Ate, twisted Ate or pairing lattices; and for every model of elliptic curve or coordinates. Especially, we expose the failure of the point blinding countermeasure to protect the Miller algorithm, main tool in pairing computation. The attack is based on solving a non linear system using Gröbner basis. As the degree of the equations in the system increase exponentially, we want to know what is the boundary between a system that can be solved and a system that can't be.

In this talk, I will present pairing-based cryptography, describe the attack against pairings and the question I have about Gröbner basis.

References

[1] N. El Mrabet, *What about Vulnerability to a Fault Attack of the Miller Algorithm During an Identity Based Protocol?*, Advances in Information Security and Assurance, LNCS 5576, pp. 122–134, 2009.

[2] N. El Mrabet and E. Fouotsa, *Failure of the Point Blinding Countermeasure against Fault Attack in Pairing-Based Cryptography* to appear in International Conference in Codes, Cryptology and Information Security, LNCS 9084, pp. 259–273, 2015.

[3] N. El Mrabet, D. Page and F. Vercauteren, *Fault Attacks in Pairing-Based Cryptography*, in Fault analysis in Cryptography, Ed. M. Joye and M. Tunstall, Springer, 2012.

[4] T. Iyama, S. Kiymoto, K. Fukushima, T. Tanaka and T. Takagi, *Efficient implementation of pairing on BREW mobile phones*, Advances in Information and Computer Security, pp. 326–336, Springer.

[5] M. Joye and G. Neven, *Identity-based cryptography*, Cryptology and information security series, IOS Press, 2009.

[6] D. Page and F. Vercauteren, *A fault attack on Pairing-based cryptography*, IEEE Tr. on Computers, v. 55, n. 9, pp. 1075–1080, 2006.

Computation of Gröbner bases and tropical Gröbner bases over p-adic fields*

Tristan Vaccon (Univ. Rennes I)

Computation of Gröbner bases over non-exact fields such as $\mathbb{R}$ or $\mathbb{Q}_p$ is a difficult task.[1] Usually, elements in such fields can only be manipulated with finite precision. Nevertheless, during the last few decades, the advent of arithmetic geometry has led to the study of varieties that are defined over $\mathbb{Q}_p$. Hence, the need to an answer to the following natural question: **which Gröbner bases over $\mathbb{Q}_p$ can be computed** (with finite precision)**?**

Direct computations through the Buchberger algorithm naturally fail because they rely on zero-testing, something that can not be achieved over p-adics. Nevertheless, we show in [6] that the Matrix-F5 algorithm[2] can be adapted so as it can compute Gröbner bases at finite precision for sequences of input homogeneous polynomials in $\mathbb{Q}_p[X_1, \ldots, X_n]$ satisfying some Zariski-open explicit regularity hypotheses. Namely, for a given monomial order ω, we ask that the input polynomials form a regular sequence and a weakly-ω ideal. Moreno-Socias has conjectured in [4] that such hypotheses are generic for any choice of degrees for the input homogeneous polynomials.

Parallelly to the previous answer, the need for explicit computations in tropical geometry has given birth to a definition of tropical Gröbner bases for ideals in $\mathbb{Q}_p[X_1, \ldots, X_n]$ that takes into account the valuation of the coefficients. Namely, instead of a monomial order, an order on the terms is used. Chan and Macalagan have proved in [2] that a Buchberger algorithm can be used to compute tropical Gröbner bases. We show in [7] that a Matrix-F5 algorithm can be adapted to compute such bases. For finite-precision computations, only the regular-sequence hypothesis is then required. Hence, generically, tropical Gröbner bases can be

[*] We report on [6] and [7]

[1] We refer to [5] for an introduction to the computation of Gröbner bases over floating-point numbers.

[2] See [3], [1].

computed at finite precision. Moreover, for some explicit special choice of term order, the numerical stability is much better than for the case of classical Gröbner bases.

References

[1] Bardet, Magali, Faugère, Jean-Charles & Salvy, Bruno On the Complexity of the F5 Gröbner basis Algorithm, Journal of Symbolic Computation, pages 1-24, September 2014.

[2] Chan, Andrew J. & Maclagan, Diane Gröbner bases over fields with valuations, arxiv:1303.0729

[3] Faugère, Jean-Charles A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In Proceedings of the 2002 international symposium on Symbolic and algebraic computation, ISSAC '02, pages 75-83, New York, NY, USA, 2002. ACM.

[4] Moreno-Socias, Guillermo Autour de la fonction de Hilbert-Samuel (escaliers d'idéaux polynomiaux), Thèse, École Polytechnique, 1991.

[5] Sasaki,T. & Kako,F. Term cancellations in computing floating-point Gröbner bases. In Proceedings of CASC 2010, volume 6244 of Lecture Notes in Comput. Sci., pages 220–231, Berlin, 2010. Springer.

[6] Vaccon, T. Matrix-F5 Algorithms over Finite-precision Complete Discrete Valuation Fields, Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation, ISSAC '14.

[7] Vaccon, T. Matrix-F5 Algorithms and Tropical Gröbner Base Computation, Proceedings of the 40th International Symposium on Symbolic and Algebraic Computation, ISSAC '15.

Modular Techniques to Compute Gröbner Bases over Non-Commutative Algebras with PBW Bases

Sharwan K Tiwari[1], Christian Eder [2], Wolfram Decker[3]

[1] *TU Kaiserslautern, Germany, stiwari@mathematik.uni-kl.de*
[2] *TU Kaiserslautern, Germany, ederc@mathematik.uni-kl.de*
[3] *TU Kaiserslautern, Germany, decker@mathematik.uni-kl.de*

In this work we present the modular techniques to compute Gröbner bases for a special class of non-commutative algebras, named as PBW algebras. The PBW algebras include many important algebras such as Weyl algebras, Universal enveloping algebras of any finite dimensional Lie algebras, Quantum algebras. Modular techniques [1] have been accepted as a powerful tool to deal with the coefficient swelling problem during the computation of Gröbner bases over commutative algebra. We have extended these techniques over PBW algebras. An implementation for the modular algorithm along with the parallelization has been carried out in the platform of computer algebra system SINGULAR[2]. In order to check the correctness of the computed Gröbner basis, the verification result for the homogeneous ideals in the homogeneous PBW algebras has also been shown. The performance of the implementation has been compared with the existing implementations in the SINGULAR.

Let $k\langle x\rangle := k\langle x_1,\dots,x_n\rangle$ be the free associative k-algebra generated by $x_1,\dots,x_n$ over the field of rationals k. We consider a graded admissible order $\preceq$ on $\mathbb{N}^n$. A monomial of the form $x^\alpha = x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ is called the standard monomial and a polynomial consists of these monomials is called the standard polynomial. We denote the largest exponent of the monomials of f by $\exp(f)\in\mathbb{N}^n$ and $Exp(G) := \{\exp(g)\mid g\in G\}$. Let us consider a finite set of relations $T = \{x_jx_i = q_{ji}x_ix_j + p_{ji} \mid 1\le i<j\le n\}$, where $q_{ji}\in k\setminus\{0\}$ and $p_{ji}\in k\langle x\rangle$ are the standard polynomials. Now consider the two sided ideal $I_T = \langle x_jx_i - q_{ji}x_ix_j - p_{ji}\rangle \subseteq k\langle x\rangle$ generated by the relations T. Then $R := k\langle x\rangle/I_T$ will be a PBW algebra with respect $\preceq$, if it satisfies the following conditions:

(i) $\exp(p_{ji}) \prec \exp(x_i)+\exp(x_j)$ for each $1\le i<j\le n$,

(ii) the set of standard monomials $x^\alpha,\ \alpha\in\mathbb{N}^n$, forms a k basis of R.

The PBW algebras have also been studied under the names as *algebras of solvable* type [3, 4, 5] and *G-algebras* [6, 7].

Using modular techniques, one computes several Gröbner bases for different primes and then lift the result to the rationals by the Chinese remainder algorithm and the Farey map. Afterwards, verify the correctness of the lifted result by the following verification test.

Theorem 1. *Let R be a homogeneous PBW algebra with respect to an admissible order $\preceq$. Let $I \subseteq R$ be a homogeneous left ideal and $G \subseteq R$ be a set of homogeneous polynomials in R such that G is a Gröbner basis of the left ideal $\langle G \rangle$, $Exp(G) = Exp(G_p)$ and G_p is a Gröbner basis of I_p for some prime p, and $I \subseteq \langle G \rangle$. Then G is a Gröbner basis of I.*

We have tested our implementation on a very interesting and challenging family of ideals from the D-module structure theory. Computing Gröbner bases of this family gives the Bernstein-Sato Polynomials. Let us consider the Weyl algebra $D_2[s] := \mathbb{Q}\{x_1, x_2, \delta_1, \delta_2, s \mid \delta_i x_i = x_i \delta_i + 1,\ \delta_i x_j = x_j \delta_i,\ i \neq j,\ \preceq\}$, where $\preceq$ is an elimination ordering, and the family of Reiffen curves $RC(p,q) := x_1^p + x_2^q + x_1 x_2^{q-1} \in \mathbb{Q}[x_1, x_2]$, where $q \geq p+1$. Now, the considered family of ideals is $BS(p,q) := \{Ann_{D_2[s]} RC^s, RC\} \subseteq D_2[s]$, where Ann denotes the annihilator. In what follows upto now, the Gröbner basis computation of $BS(6,7)$ is feasible, while our new modular approach can compute the Gröbner basis of $BS(7,8)$ as well.

We have also tested the performance of our implementation on the homogeneous polynomials of cyclic(8) (qc_cyclic(8)), and the katsura(10) polynomials (qc_katsura(10)), from the quasi commutative algebra $R := \mathbb{Q}\{x_1, \ldots, x_n \mid x_j x_i = 2x_i x_j,\ 1 \leq i < j \leq n,\ \preceq\}$, where $\preceq$ is the degree reverse lexicographic ordering.

The following table gives the timings of the modular algorithm compared to the *slimgb* and the *std* implementations of the SINGULAR, for the above mentioned examples. If the computation does not terminate successfully within 25 days or it is killed because of huge memory requirement (more than 150 GB), then this computation is denoted by ∞ in the table. In the following, letters *h*, *m*, *s* and string *thr* denote hours, minutes, seconds and threads respectively.

Table 1: Performance of modular algorithm versus std and slimgb:

Ex	std	slimgb	modular algorithm				
			1 *thr*	2 *thr*	4 *thr*	8 *thr*	16 *thr*
BS(5,6)	∞	63.86 *h*	12.25 *m*	7.21 *m*	4.70 *m*	3.45 *m*	2.60 *m*
BS(6,7)	∞	∞	6.50 *h*	6.03 *h*	4.65 *h*	4.24 *h*	3.54 *h*
qc_cyclic(8)	∞	48.12 *h*	52.78 *m*	29.2 *m*	22 *m*	23.01 *m*	17.50 *m*
qc_katsura(10)	50.28 *m*	1.01 *h*	6 *s*	5.10 *s*	3.90 *s*	3.20 *s*	5.40 *s*

References

[1] Arnold, E. A.: *Modular algorithms for computing Gröbner bases.* J. Symbolic Computation Vol. 35, pp. 403–419 (2003).

[2] Decker, W.; Greuel, G.-M.; Pfister, G.; Schönemann, H.: SINGULAR 4-0-1 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de (2014).

[3] Kandri–Rody, A.; Weispfenning, V.: *Non–commutative Gröbner bases in algebras of solvable type.* J. Symbolic Computation, 9(1):1–26 (1990).

[4] Kredel, H.: *Solvable polynomial rings.* Shaker (1993).

[5] Levandovskyy, V.; Schönemann, H.: *Noncommutative Gröbner bases and filtered–graded transfer.* Springer(2002).

[6] Levandovskyy, V.; Schönemann, H.: *Plural- a computer algebra system for non-commutative polynomial algebras.* In Proc. of the international and Symposium on symbolic and algebraic computation(ISSAC' 03), ACM Press (2003).

[7] Mora, T.: *Gröbner Bases in non–commutative Algebras.* In: Proc. of the International Symposium on Symbolic and Algebraic Computation (ISSAC '88), 150–161, LNCS 358 (1989).

Efficient Groebner bases computation for $\mathbb{Z}[x]$ lattice

Chun-Ming Yuan
Academy of Mathematics and System Sciences
Chinese Academy of Sciences

In this talk, we give two algorithms to compute the Groebner Bases for $\mathbb{Z}[x]$-lattice. The first one is based on the Hermite normal form computation on $\mathbb{Z}^n$. The second one is a modular algorithm, use the properties of reduced Groebner bases for $\mathbb{Z}[x]$ lattice. The main difference with the traditional modular algorithm is that we use the unlucky primes. Experimental results show that these two algorithms are more efficient than the tradictional Algorithm.

Solving Polynomial Systems Using the Dixon-EDF Resultant with Emphasis on Image Analysis Problems

Robert H. Lewis

Fordham University, New York, NY 10458, USA
http://fordham.academia.edu/RobertLewis
Google: Robert Lewis Fordham

Using examples of interest from real problems, we will discuss the Dixon-EDF resultant as a method of solving parametric polynomial systems that arise in image analysis or geometry. We will briefly describe the method itself, then discuss a new approach to a classic problem called the "six-line problem". We also discuss flexibility of structures, pose estimation, and surface reconstruction from point clouds. We will compare Dixon-EDF to several implementations of Gröbner bases algorithms on several systems. We find that Dixon-EDF is greatly superior.

Keywords: polynomial system, parameter, resultant, Dixon, determinant, symbolic computing, Gröbner basis.

Solving polynomial system with linear univariate representation

Jinsan Cheng
Academy of Mathematics and System Sciences
Chinese Academy of Sciences

In this talk, we will show an improved local generic position method for isolating the roots of a zero-dimensional bivariate polynomial system with two polynomials and extend the method to general zero-dimensional polynomial systems. The method mainly involves resultant computation and root isolation of univariate polynomial equations. Our implementation considers only real roots. It is probability 1 correct. The implementation shows that the method is efficient, especially for bivariate polynomial systems.

Joined work with Kai Jin.

About Triangular Matrix Decomposition in Domain

Gennadi Malaschonok and Anton Scherbinin
Tambov State University, Tambov, Russia
malaschonok@ya.ru

Abstract

We suggest deterministic recursive algorithm for the computation of the new form of triangular matrix decompositions. It can be viewed as a generalization of $PLUQ$ and Bruhat decompositions in domain.

We suggest deterministic recursive algorithm for the computation of triangular matrix decompositions with permutations like $PLUQ$ and Bruhat decomposition. It based on [1] and [2]. Let R – commutative domain, $A \in R^{n \times m}$ is a matrix. New triangular decomposition has form $A = PLDUQ$, where $D \in R^{n \times m}$ is the diagonal matrix, which rank is equal the rank of matrix A, P and Q - the permutation matrices and L and U - the lower and upper triangular matrices. It can be viewed as a generalization of $PLUQ$ and Bruhat decompositions, it also summarizes the cases of complete and incomplete rank. Let S be the "fipped" identity matrix, $PLDUQ$ be triangular decomposition for the matrix SA, then Bruhat decomposition can be writen as follow:

$$A = \mathbf{VwU} = (SPLD_1P^TS)(S^TPI^r_{n,m}Q)(Q^TD_2UQ),$$

$$\text{where } D = D_1I^r_{n,m}D_2,$$

$$D_1 = \mathbf{diag}((a^1)^{-1}, .., (a^r)^{-1}, 0, .., 0), \; D_2 = \mathbf{diag}(1, (a^1)^{-1}, .., (a^{r-1})^{-1}, 0, .., 0).$$

Here a^i - is a sequence of non-zero minors of A of size i. Algorithm have the same complexity as the algorithm of matrix multiplication.

References

[1] Malaschonok, G.I. *Fast generalized Bruhat decomposition.* In: Ganzha, V.M., Mayr, E.W., Vorozhtsov, E.V. (eds.) Computer Algebra in Scientific Computing. CASC'2010, LNCS 6244. Springer, Berlin, (2010), 194-202.

[2] Malaschonok G.I. *Generalized Bruhat decomposition in commutative domains.* In: Computer Algebra in Scientific Computing. CASC'2013. LNCS 8136, Springer, Heidelberg, (2013), 231-242.

Polynomial-Time Algorithms for Quadratic Isomorphism of Polynomials: The Regular Case

J. Berthomieu, J.-C. Faugère, L. Perret
Sorbonne Universités, UPMC Univ Paris 06, Équipe PolSys, LIP6
CNRS UMR 7606, LIP6
INRIA, Équipe PolSys, Centre Paris – Rocquencourt
jeremy.berthomieu@lip6.fr,
jean-charles.faugere@inria.fr,
ludovic.perret@lip6.fr

Let $\mathbb{K}$ be a field and $\mathbf{x} = (x_1, \ldots, x_n)$ indeterminates. Let $\mathbf{f} = (f_1, \ldots, f_m)$ and $\mathbf{g} = (g_1, \ldots, g_m)$ be two sets of $m \geq 1$ homogeneous polynomials in $\mathbb{K}[\mathbf{x}]$. We considere the problem of computing – if any – a matrix $A \in \mathrm{GL}_n(\mathbb{K})$ such that $\mathbf{f}(A\cdot\mathbf{x}) = \mathbf{g}(\mathbf{x})$. This fundamental problem has many applications and is called *Isomorphism of Polynomials with one Secret* (IP1S). Amongst its applications, we can cite *Graph Isomorphism* (GI) which reduces to equivalence of cubic polynomials with respect to an invertible linear change of variables, according to Agrawal and Saxena [1], mutivariate cryptosystems, reduction of circuits in algebraic complexity... We can also note that if $m = 1$ and f_1, g_1 have degree 2, then IP1S is easily solved using Gauss's quadratic forms reduction algorithm.

Equivalence of multivariate polynomials is also a fundamental problem in Multivariate Public-Key Cryptography (MPKC). This is a family of asymmetric (encryption and signature) schemes whose public-key is given by a set of m multivariate equations ([6, 7]). To minimize the public-key storage, the multivariate polynomials considered are usually quadratic. The basic idea of MPKC is to construct a public-key which is equivalent to a set of quadratic multivariate polynomials with a specific structure (see for instance [8]).

In computer algebra, a problem close to IP1S is the simplification of a polynomial system $\mathbf{f}$: compute $A \in \mathrm{GL}_n(\mathbb{K})$ such that $\mathbf{g}(\mathbf{x}) = \mathbf{f}(A\cdot\mathbf{x})$ is easier to solve. In this light, Ridge [3] and MinVar [4] algorithms reduce as much as possible the number of variables of the considered system. More generaly, given $\mathbf{f}$, the *Functional Decomposition Problem* consists in computing homogeneous $\mathbf{h} = (h_1, \ldots, h_s)$ and $\mathbf{g}$ such that $\mathbf{f}(\mathbf{x}) = \mathbf{g}(\mathbf{h}(\mathbf{x}))$.

In this talk, we present a probabilistic polynomial-time algorithm for solving regular quadratic instances of IP1S with m any [2]. Let $H_1, \ldots, H_m$ be the matrix representations of the f_i's, with $\operatorname{char}\mathbb{K} \neq 2$. A quadratic instance shall be called *regular* if there exists a linear combination of the H_i's with maximal rank. This improves the results obtained up to now since the algorithms were either heuristic, with potentially non polynomial-time complexity, or dedicated to special case as $m = 2$.

Let $H_1', \ldots, H_m'$ be the matrix representations of $g_1, \ldots, g_m$. Solving the equivalence problem between $\mathbf{f}$ and $\mathbf{g}$ comes down to computing A invertible such that

$$A^{\mathrm{T}}\, H_i\, A = H_i', \quad \forall i,\ 1 \leq i \leq m.$$

We show that we can essentially *linearize* the problem by reducing quadratic-IP1S to test the orthogonal simultaneous similarity of symmetric matrices, *i.e.* to solve

$$A^{\mathrm{T}}\, A = \mathrm{Id}_n, \quad H_i\, A = A\, H_i', \quad \forall i,\ 2 \leq i \leq m.$$

Chistov, Ivanyos and Karpinski [5] showed that the latter problem is equivalent to computing an invertible matrix in a subspace of $\mathbb{K}^{n\times n}$ and to compute a square root. While computing square roots of matrices can be done efficiently using numerical methods, it seems difficult to control the bit complexity of such methods. Indeed, if $\mathbb{K} = \mathbb{Q}$, the square root may only exist in an extension of $\mathbb{K}$ of degree exponential in n. However, we present exact and polynomial-time algorithms for computing a representation of the square root of a matrix in $\mathbb{K}^{n\times n}$, for various fields (including finite fields), as a product of two matrices. This representation allows us to deduce if $\mathbf{f}$ and $\mathbf{g}$ are equivalent.

Finally, we give experiments results wherein we solve instances whose sizes are an order of magnitude bigger than cryptographic *challenges*.

Bibliographie

[1] M. Agrawal and N. Saxena, 2006. Equivalence of F-Algebras and Cubic Forms. In: B. Durand, W. Thomas (Eds.), STACS. Vol. 3884 of Lecture Notes in Computer Science. Springer, pp. 115–126.

[2] J. Berthomieu, J.-C. Faugère and L. Perret, 2014. Polynomial-Time Algorithms for Quadratic Isomorphism of Polynomials: The Regular Case. Preprint, `http://hal.inria.fr/hal-00846041`.

[3] J. Berthomieu, P. Hivert and H. Mourtada, 2010. Computing Hironaka's invariants: Ridge and Directrix. In: Arithmetic, Geometry, Cryptography and Coding Theory 2009. Vol. 521 of Contemp. Math. Amer. Math. Soc., Providence, RI, pp. 9–20.

[4] E. Carlini, 2005. Reducing the number of variables of a polynomial. In: Algebraic geometry and geometric modeling. Springer, pp. 237–247.

[5] A. L. Chistov, G. Ivanyos and M. Karpinski, 1997. Polynomial time algorithms for modules over finite dimensional algebras. In: B. W. Char, P. S. Wang, W. Küchlin (Eds.), ISSAC. ACM, pp. 68–74.

[6] Matsumoto, T., Imai, H., 1988. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In: Advances in Cryptology – EUROCRYPT 1988. Vol. 330 of LNCS. Springer–Verlag, pp. 419–453.

[7] Patarin, J., 1996. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In: Maurer, U. M. (Ed.), EUROCRYPT. Vol. 1070 of Lecture Notes in Computer Science. Springer, pp. 33–48.

[8] Wolf, C., Preneel, B., 2011. Equivalent keys in multivariate quadratic public key systems. Journal of Mathematical Cryptology 4 (4), 375–415.

Computational Aspects and Mathematical Methods for Finite Fields

Session Organizers

Kenza Guenda
ATN, Faculty of Mathematics, USTHB
ken.guenda@gmail.com

Ilias Kotsireas
Department of Physics and Computer Science
Wilfrid Laurier University
ikotsire@wlu.ca

Sihem Mesnager
LAGA, Department of Mathematics
Paris 8 University and Telecom ParisTech France
smesnager@univ-paris8.fr

Overview

The session will cover general technical aspects of finite fields and their applications in communications, cryptography, coding theory and combinatory.

The aim of this session is to bring together researchers from several aspects of finite fields : computation and applications. Topics of interest include, but are not limited to : Computational aspects of finite fields algorithms and complexity, polynomial factorization, decomposition and irreducibility testing, estimation and computation character sums, finding primitive and other special elements of finite fields, algorithms for polynomials, curves, varieties, sequences and functions over finite fields, Gröbner Basis.

A characterization of MDS codes that have an error correcting pair

Irene Márquez-Corbella[1], Ruud Pellikaan[2]

[1] *SECRET of INRIA, Rocquencourt, France. E-mail: irene.marquez-corbella@inria.fr*
[2] *Dept. of Mathematics, Eindhoven University of Technology. E-mail: g.r.pellikaan@tue.nl*

1 abstract

Error-correcting pairs (ECP) were introduced in [6, 8] and independently in [3] as a general algebraic method of decoding linear codes. These pairs exist for several classes of codes such as for generalized Reed-Solomon, cyclic, alternant and algebraic geometry codes [1, 2, 3, 4, 7, 8, 9]. However little or no study has been made for characterizing those codes. This article is an attempt to fill the vacuum left by the literature concerning this subject. The aim of this paper is to characterize those t-error correcting MDS codes that have a t-error correcting pair. Since every linear code is contained in an MDS code of the same minimum distance over some finite field extension, see [9], we have focused our study on the class of $[n, n-2t, 2t+1]$ codes with a t-ECP. It turns out to be the class of generalized Reed-Solomon codes. This was shown for $t \leq 2$ in [9].

We will give the back round of MDS codes. Generalized Reed-Solomon codes and an equivalent way to describe such a code as a projective system on a rational normal curve in projective space is reviewed. A classical result is stated that a rational rational curve in projective r space is uniquely determined by n of its points in case $n \geq r+2$. This classical result will be vital in our main result.

For further details on the notion of an error correcting pair we formally review this definition, detailing the state-of-art and the existence of error correcting pair for some families of codes. Also a survey of well-known results related to generalized Reed-Solomon codes which would be used to set the notation and recall some properties that are relevant for the proof of the main result.

Finally, we present the main result of this paper that states that every MDS code with minimum distance $2t+1$ and having a t-ECP belongs to the class of generalized Reed-Solomon codes. A second proof is given using a recent results [5, 10] on the Schur product of codes.

References

[1] I.M. Duursma, *Decoding codes from curves and cyclic codes*, PhD Thesis, Eindhoven University of Technology (1993).

[2] I.M. Duursma and R. Kötter, *Error-locating pairs for cyclic codes*, IEEE Trans. Inform. Theory **40**, pp. 1108–1121 (1994).

[3] R. Kötter, *A unified description of an error locating procedure for linear codes*, Proceedings of Algebraic and Combinatorial Coding Theory, Voneshta Voda, pp. 113–117 (1992).

[4] R. Kötter, *On algebraic decoding of algebraic-geometric and cyclic codes*, PhD Thesis, Linköping Studies in Science and Technology, Dissertation no. **419**, (1996).

[5] D. Mirandola and Z. Gilles,*Critical pairs for the product singleton bound*, arXiv:1501.06419 (2015).

[6] R. Pellikaan,*On decoding linear codes by error correcting pairs* Preprint Eindhoven University of Technology, 1988.

[7] R. Pellikaan, *On a decoding algorithm of codes on maximal curves*, IEEE Trans. Inform. Theory **35**, pp. 1228–1232 (1989).

[8] R. Pellikaan, *On decoding by error location and dependent sets of error positions*, Discrete Math. **106–107**, pp. 369–381 (1992).

[9] R. Pellikaan, *On the existence of error-correcting pairs*, Statistical Planning and Inference **51**, pp. 229–242 (1996).

[10] H. Randriambololona, *An upper bound of singleton type for componentwise products of linear codes*, IEEE Trans. Inform. Theory **59**, 12, pp. 7936–7939 (2013).

Simplex and MacDonald Codes over R_q

K. Chatouh, K. Guenda, T. A. Gulliver and L. Noui

07-06-2015

Key Words: Simplex codes, MacDonald codes, Gray map, Codes over rings, Lee weight, Homogeneous weight.

Although codes over rings are not new, they have attracted significant attention from the scientific community only since 1994, when Hammons et al. [6] established a fundamental connection between non-linear binary codes and linear codes over $\mathbb{Z}_4$. In [6], it was proven that some of the best non-linear codes, such as the Kerdock, Preparata, and Goethal codes can be viewed as linear codes over $\mathbb{Z}_4$ via the Gray map from $\mathbb{Z}_4^n$ to $\mathbb{F}_2^{2n}$. Many of their results have been extended to finite chain rings such as Galois rings and rings of the form $\mathbb{F}_2[u]/\langle u^m \rangle$. Recently, as a generalization of previous studies [8, 9], Dougherty et al. [2] considered codes over an infinite class of rings, denoted R_q. These rings are finite and commutative Frobenius rings, but are not finite chain rings. The ring R_q is with a unique maximal ideal which consists of all non-units elements. Since the work of Nechaev and Hohold [7] it is well known that each Finite Frobenuis Commutative ring has a Homogeneous weight. The difficulty is in finding this weight. Recently [10] defined the Homogeneous weight and a Gray map over the ring R_q. In this paper we give a different Homogeneous weight as well as its Gray map the rings R_q. Further, we define the simplex codes and MacDonald codes of type α and β over these ring. We study many of their properties, as well as their binary images. Our motivations in studying such codes comes form the fact that these codes are with few weights. They also find some other applications such as PSK modulation and some cryptographic purposes.

References

[1] S.T. Dougherty, T.A. Gulliver, and J. Wong, *Self-dual codes over $\mathbb{Z}_8$ and $\mathbb{Z}_9$*, Designs, Codes, Crypt., 41, pp. 235–249, 2006.

[2] S.T. Dougherty, B. Yildiz, and S. Karadeniz, *Codes over R_k, Gray maps and their binary images*, Finite Fields Appl., vol. 17, no. 3, pp. 205–219, May 2011.

[3] M. Greferath and S. E. Schmidt, *Finite-ring combinatorics and MacWilliams equivalence theorem*, J. Combin. Theory Ser. A, 92, pp. 17–28, 2000.

[4] M.K. Gupta, D.G. Glynn, and T.A. Gulliver, *On senary simplex codes*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Computer Science, vol. 2227, pp. 112–121, 2001.

[5] M.K. Gupta, *On Some Linear Codes over* $\mathbb{Z}_{2^s}$, Ph.D. Thesis, IIT Kanpur, 1999.

[6] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Solé, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory, vol. 40, pp. 301–319, 1999.

[7] A.A. Nechaev and T. Honold, *Fully weighted modules and representations of codes*, Problemy Peredachi Informatsii 35, no. 3, pp. 1839, 1999.

[8] B. Yildiz and S. Karadeniz, *Linear codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Designs, Codes, Crypt., vol. 54, no. 1, pp. 61–81, 2010.

[9] B. Yildiz and S. Karadeniz, *Cyclic codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Designs, Codes, Crypt., vol. 58, no. 1, pp. 221–234, 2011.

[10] B. Yildiz and I.G. Kelebek, *The homogeneous weight for* R_k*, related Gray map and new binary quasicyclic codes*, arXiv:1504.04111v1 [cs.IT] 16 Apr 2015.

Algebraic Modelling of Covering Arrays

Bernhard Garn[1] and Dimitris E. Simos[1]

[1] *SBA Research, Vienna, Austria, {bgarn, dsimos}@sba-research.org*

A *Covering Array* (CA) is a mathematical object that is well suited to do hardware and software testing given that optimal ones provide minimal cardinality (i.e. minimum number of tests) with maximal coverage (i.e. that all interactions of certain size are covered at least once). Formally a *Covering Array* is defined by four positive integers N (number of rows or tests), t (the strength or size of interactions that are covered), k (the number of factors or variables), and v (the alphabet of the *Covering Array*), and is denoted by $\mathrm{CA}(N;t,k,v)$ that is an $N \times k$ array $A = (a_{i,j})$, $0 \leq i \leq N-1$, $0 \leq j \leq k-1$, over $\mathbf{Z}_v = \{0,1,\ldots,v-1\}$ with the property that for any t distinct columns $0 \leq c_0 < c_1 \cdots < c_{t-1} \leq k-1$, and any member $(x_0,x_1,\ldots,x_{t-1})$ of $\mathbf{Z}_v^t$, there exists at least one row r such that $x_i = a_{r,c_i}$ for all $0 \leq i \leq t-1$. For a general overview of *Covering Arrays* we refer to [3].

Starting from the early 2000s, *Covering Arrays* have become *en vogue* in new application domains, one important being software testing [5] and in particular combinatorial testing. Currently, there are approaches to extend these testing methods to applications of information security [1]. The fact that a (possibly not optimal) *Covering Array* always exists is a major advantage in contrast to *Orthogonal Arrays* and the constraints regarding their parameter values.

The literature has seen a lot of approaches used to construct *Covering Arrays*, based for example on algebraic (AETG) and different optimization strategies (genetic algorithms, simulated annealing, etc.). This shift towards the usage of optimization strategies, which should provide sufficiently optimized solutions, to construct *Covering Arrays*, is an important step towards their practical applicability, where one is faced with very different requirements regarding their parameters. This extends the historically longer application of combinatorial designs in statistics, coding theory and telecommunications.

Furthermore, multiple recursive constructions have been given in the literature, however, with some of them relying on a specific choice of the parameters t, k and v to be applicable. To give another practical example from combinatorial testing relating to these theoretical methods, it can be the case that one is faced with the task to extend a given legacy test suite to a *Covering Array* to employ pairwise-testing, or to add a new parameter to a given test suite and similarly create a strength two *Covering Array* [4]. Akin strategies are also employed internally in the algorithms of the IPO-family [6], were such extension strategies are referred to as vertical and horizontal extension, respectively. In these intermediate construction steps a choice has to be made under the constraint to maximize the achieved coverage. For this task, special heuristics and data structures have been developed.

In this talk, we are interested in modelling the necessary coverage criteria with techniques that are derived from an algebraic perspective. We will use algebraic notions like inner products in vector spaces, symbolic computation and Gröbner bases [2] to illustrate our approach. This represents a new point of view with regard to a new formalism for the properties of *Covering Arrays*, combining practical application requirements with the aforementioned tools of computer algebra and symbolic computation. As future work, we want to develop an algebraic framework to identity, characterize and build *Covering Arrays*.

Acknowledgements. This work was supported by the COMET K1 program by the Austrian Research Funding Agency (FFG).

References

[1] BOZIC, J., GARN, B., SIMOS, D. E., AND WOTAWA, F. Evaluation of the IPO-family algorithms for test case generation in web security testing. In *Software Testing, Verification and Validation Workshops (ICSTW), 2015 IEEE Eighth International Conference on* (April 2015), pp. 1–10.

[2] BUCHBERGER, B. Bruno buchberger's phd thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *J. Symb. Comput. 41* (March 2006), 475–511.

[3] COLBOURN, C. J. Covering arrays. In *Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds., 2nd ed., Discrete Mathematics and Its Applications. CRC Press, Boca Raton, Fla., 2006, pp. 361–365.

[4] HARTMAN, A., AND RASKIN, L. Problems and algorithms for covering arrays. *Discrete Mathematics 284*, 1–3 (2004), 149 – 156.

[5] KUHN, D., AND REILLY, M. An investigation of the applicability of design of experiments to software testing. In *Software Engineering Workshop, 2002. Proceedings. 27th Annual NASA Goddard/IEEE* (Dec 2002), pp. 91–95.

[6] LEI, Y., KACKER, R., KUHN, D., OKUN, V., AND LAWRENCE, J. Ipog: A general strategy for t-way software testing. In *Engineering of Computer-Based Systems, 2007. ECBS '07. 14th Annual IEEE International Conference and Workshops on the* (March 2007), pp. 549–556.

ON THE DIOPHANTINE EQUATION $1 + 5x^2 = 3y^n$

ABDELKADER HAMTTAT AND DJILALI BEHLOUL

Abstract. The purpose of this paper is to give all solutions of the Diophantine equation $1 + 5x^2 = 3y^n$, for almost values of n.

1. Introduction

We start by the important fact that Diophantine equations have many applications in coding theory (see[5]) and modern cryptography (see[4]).

The Diophantine equation $x^2 + C = y^n$, in positive integers unknowns x, y and n, has a long story. The first case to have been solved appears to be $C = 1$. In 1850 Victor Lebesgue showed, using a elementary factorization argument, that the only solution is $x = 0$, $y = 1$. Over the next 140 years many equations of the form $x^2 + C = y^n$ have been solved using the Lebesgue's elementary trick. In 1993 John Cohn published an exhautive historical survey of this equation which completes the solution for but all 23 values of C in the range $1 \leq C \leq 100$.

It has been noted recently, that the result of Bilu, Harnot and Voutier can sometimes be applied to equations of the form $x^2 + C = y^n$, when instead of C being a fixed integer, C is the product of powers of fixed primes $p_1, ..., p_k$.

By comparison, The Diophantine equation $x^2 + C = 2.y^n$ with the same restriction, has been solved partially. For $C = 1$, John Cohn, showed that the only solutions to this equation are $x = y = 1$ and $x = 239$, $y = 13$ and $n = 4$. SZ. Tengely studied the equation $x^2 + q^{2m} = 2.y^p$ where x, y, q, p, m are integers with $m > 0$ and p, q are odd primes and $\gcd(x, y) = 1$. He proved that there are only finitely many solutions (m, p, q, x, y) for which y is not a sum of two consecutive squares. He also studied the equation for fixed q and resolved it when $q = 3$. In 2007, F. S. Abu Muriefah, F. Luca, S. Siksek, and SZ. Tengely give a very sharp bound for prime values of the exponent n, when $C \equiv 1(\bmod 4)$. When $C \not\equiv 1(\bmod 4)$ they explain how the equation can be solved using the multi-Frey variant of the modular approach. They illustrate their approach by solving completely the equations $x^2 + 17^{a_1} = 2y^n$, $x^2 + 5^{a_1}.13^{a_2} = 2y^n$ and $x^2 + 3^{a_1}.11^{a_2} = 2y^n$.In 2009, F. Luca, S. Tengely, and A. Togbe give all solutions of that the equation $x^2 + C = 4y^n$ when $\gcd(x, y) = 1$, $C \equiv 3(\bmod 4)$ and $1 \leq C \leq 100$.

The aim of this work is to solve the Diophantine equation $1 + 5x^2 = 3y^n$, for almost values of $n \geq 2$.

2. Results

Considering the following equation

Date: May 04, 2015.

$$1+5x^2=3y^n \tag{2.1}$$

in integer unknowns x, y, n satisfying

$$x \in \mathbb{Z}, \quad y \geq 1 \text{ and } 2 \leq n \leq 5 \tag{2.2}$$

Theorem 1. *Consider the equation (2.1) satisfying (2.2) .Then the only solution of equation (2.2) is* $(x, y, n) = (\pm 4, 3, 3)$.

2.1. **Auxiliary results.** To prove theorem (1), we need the following result

Theorem 2. *Let C be a positive integer satisfying* $C \equiv 1 (\bmod 4)$, *and write* $C = cd^2$, *where c is a square- free. Suppose that (x, y) is a solution of the equation*

$$x^2 + C = 2y^p, \qquad x, y \in \mathbb{Z}^+, \qquad \gcd(x, y) = 1,$$

where $p \geq 5$ is a prime , then either
i) $x = y = C = 1$, or
ii) p divides the class number of the quadratic field $\mathbb{Q}(\sqrt{-c})$, or
iii) $p = 5$ and $(C, x, y) = (9, 79, 5), (125, 19, 3), (125, 183, 7), (2125, 21417, 47)$, or
iv) $p \mid (q - (-c \mid q))$, where q is some odd prime such that $q \mid d$ and $q \nmid c$. here $(c \mid q)$ denotes the Legendre symbol of the integer c with respect to the prime q.

Proof. See (6). □

2.2. **Proof of theorem 1.** We follow the notation from the statement of the theorem (1). We take $n = p$ a prime, p does not divide the class number of the field $\mathbb{Q}(\sqrt{-5})$. Considering equation (2.1) modulo 4 reveals that x is even and y odd. We work first in $\mathbb{Q}(\sqrt{-5})$. Since $5 \equiv 1 (\bmod 4)$, this has ring of integers $\Re = \mathbb{Z}\left[\sqrt{-5}\right]$. Factoring the left hand of (2.1), we get

$$(\pm 1 + x\sqrt{-5})(\pm 1 - x\sqrt{-5}) = 3y^p \tag{2.3}$$

multiplying both sides by 4, we obtain

$$(\pm 2 + 2x\sqrt{-5})(\pm 2 - 2x\sqrt{-5}) = 2(1+\sqrt{-5})(1-\sqrt{-5})y^p$$

and this equation becomes

$$\left(\frac{\pm 2 + 2x\sqrt{-5}}{1+\sqrt{-5}}\right)\left(\frac{\pm 2 - 2x\sqrt{-5}}{1-\sqrt{-5}}\right) = 2y^p \tag{2.4}$$

We put

$$\pi = \left(\frac{\pm 2 + 2x\sqrt{-5}}{1+\sqrt{-5}}\right) = \begin{cases} \left(\frac{5x+1}{3}\right) + \left(\frac{x-1}{3}\right)\sqrt{-5}, & \text{if } x \equiv 1 (\bmod 3), \\ \left(\frac{5x-1}{3}\right) + \left(\frac{x+1}{3}\right)\sqrt{-5}, & \text{if } x \equiv 2 (\bmod 3) \end{cases}$$

It is clear that the π is a principal ideal in $\mathbb{Z}\left[\sqrt{-5}\right]$, then $\pi = \left(U + V\sqrt{-5}\right)$ for some odd coprime integers U, V. Then the equation (2.4) becomes

$$\pi.\overline{\pi} = 2y^p$$

which implies

$$U^2 + 5V^2 = 2y^p$$

Using the theorem (2), with $c = 5$ and $d = V$, then this equation has solution if the statement (iv) holds if $p \geq 5$, so $p \mid q \pm 1$ for some prime q such that $q \mid V$ and $q \nmid 5$. If $q = 3$,7 then $p = 2, 3$. Contradiction with the fact that $p \geqslant 5$.

If $q = 11$ then $p = 5$, but it is easy to check modulo 11, that (2.1) has no solution. We conclude that (2.1) has no solution for all $n \equiv 0 \pmod 5$.

Now we take $n = p = 3$, the equation (2.1) becomes

$$1 + 5x^2 = 3y^3 \tag{2.5}$$

using the same argument in the proof for $p \geq 5$,we get

$$\pi.\overline{\pi} = 2y^3$$

We have $(2) = \boldsymbol{q}^2$ where $\boldsymbol{q}$ is a prime ideal of $\Re$. It is clear that the principal ideals $\pi, \overline{\pi}$ have $\boldsymbol{q}$ as their greatest common factor. From (2.5) we deduce that

$$\pi.\Re = \boldsymbol{q}.\boldsymbol{a}^3$$

where $\boldsymbol{a}$ is some ideal of $\Re$. Now multiply both sides by (2). We obtain

$$2.\pi = (\boldsymbol{q}.\boldsymbol{a})^3$$

Since $\gcd(h, 3) = 1$, where h is the class number of the field $\mathbb{Q}(\sqrt{-5})$, we see that $\boldsymbol{q}.\boldsymbol{a}$ is a principal ideal. Moreover, the units of $\mathbb{Q}(\sqrt{-5})$ are ± 1. Hence

$$2.(U + V\sqrt{-5}) = (a + b\sqrt{-5})^3$$

For some odd integers a, b. Moreover $y = (a^2 + 5b^2)/2$. From the coprimality of x and y, we see that a and $5b$ are coprime. equating real and imaginary parts, we get

$$\begin{cases} 2U = a(a^2 - 15b^2) \\ 2V = b(3a^2 - 5b^2) \end{cases} \tag{2.6}$$

but $U = 5V \pm 2$,then (2.6) becomes

$$a^3 - 15a^2b - 15ab^2 + 25b^3 = \pm 4$$

which is a Thue type equation with only solutions $(a, b) = (1, 1), (-1, -1)$.

so $U = \pm 7$ that means $x = \pm 4$ and $y = 3$.We conclude that (2.1) has no solution for all $n \equiv 0 \pmod 3$ and $n > 3$.

Now, we take $n = p = 2$, considering the equation (2.1) modulo 4, in one hand we get $1 + 5x^2 \equiv 1, 2 (\bmod 4)$, and in another we get $3y^2 \equiv 0, 3 (\bmod 4)$, we conclude that (2.1) has no solution for all $n \equiv 0 \pmod 2$.

Conjecture 1. *We claim that (2.1) has no solution for all* $n \geqslant 7$*, when* $n \not\equiv 0 \pmod 5$*,* $n \not\equiv 0 \pmod 3$ *and* $n \not\equiv 0 \pmod 2$*.*

Bibliography

[1] J. Cohn. The Diophantine equation $x^2 + C = y^n$. Acta Arith. 65 (1993), no.4, 367-381.

[2] V. A. Lebesgue. Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$. N.A.Math. 9 (1850), 178–181.

[3] L. Tao. On the Diophantine equation $x^2 + 5^m = y^n$. Ramanujan J. 19 (2009) 325–338.

[4] Mohammad Bagheri & al. A public -key cryptosystem besed on Diophantine equations. International Journal of Pure and Applied Mathematics. Volume 5 No. 2 2003, 135-140.

[5] Nikos Tzanakis. The Diophantine equation $x^2 = 4q^{\frac{a}{2}} + 4q + 1$, with an application to coding theory. Journal of Number Theory. Volume 26, Issue 1, May 1987, Pages 96–116.

[6] S.Siksek and al. On the diophantine equation $x^2 + C = 2y^n$. International Journal of Number Theory 5 (2009), 1117-1128.

A.T.N Laboratory, USTHB, ALGERIA
E-mail address: ahamttat@gmail.com

A.T.N Laboratory, USTHB, ALGERIA
E-mail address: dbehloul@yahoo.fr

On defining generalized rank weights

Relinde Jurrius[1], Ruud Pellikaan[2]

[1] *Institut de Mathémathiques, Université de Neuchátel. E-mail: relinde.jurrius@unine.ch*
[2] *Dept. of Mathematics, Eindhoven University of Technology. E-mail: g.r.pellikaan@tue.nl*

1 Introduction

Error-correcting codes with the rank distance were introduced by Gabidulin [4]. Recently they have gained a lot of interest because of their application to network coding. In network coding, messages are not transmitted over a single channel, but over a network of channels. This application induced a lot of theoretical research to rank metric codes.

Many notions in the theory for codes with the Hamming metric have an equivalent notion for codes with the rank metric. We studied the rank-metric equivalent of the weight enumerator and several generalizations of it [6]. From this theory, a definition of the generalized rank weights follows. These are the rank metric equivalence of the generalized Hamming weights.

This paper investigates the generalized rank weights of a code over L, where L is a finite Galois extension of a field K. This is a generalization of the case where $K = \mathbb{F}_q$ and $L = \mathbb{F}_{q^m}$ of Gabidulin codes [4] to arbitrary characteristic as considered by Augot-Loidreau-Robert [1, 2].

We show equivalence to previous definitions, in particular the ones by Kurihara-Matsumoto-Uyematsu [8, 9], Oggier-Sboui [10] and Ducoat [3].

2 Rank metric codes and weights

Let K be a field and let L be a finite Galois extension of K. A *rank metric code* is an L-linear subspace of L^n. To all codewords we associate a matrix as follows. Choose a basis $B = \{\alpha_1, \dots, \alpha_m\}$ of L as a vector space over K. Let $\mathbf{c} = (c_1, \dots, c_n) \in L^n$. The $m \times n$ matrix $M_B(\mathbf{c})$ is associated to $\mathbf{c}$ where the j-the column of $M_B(\mathbf{c})$ consists of the coordinates of c_j with respect to the chosen basis: $c_j = \sum_{i=1}^m c_{ij}\alpha_i$. So $M_B(\mathbf{c})$ has entries c_{ij}.

The K-linear row space in K^n and the rank of $M_B(\mathbf{c})$ do not depend on the choice of the basis B, since for another basis B' there exists an invertible matrix A such that $M_B(\mathbf{c}) = AM_{B'}(\mathbf{c})$. The rank weight $\mathrm{wt}_R(\mathbf{c}) = \mathrm{rk}(\mathbf{c})$ of $\mathbf{c}$ is by definition the rank of the matrix $M_B(\mathbf{c})$, or equivalently the dimension over K of the row space of $M_B(\mathbf{c})$. This definition follows from the rank distance, that is defined by $d_R(\mathbf{x}, \mathbf{y}) =$

$\text{rk}(\mathbf{x}-\mathbf{y})$. The rank distance is in fact a metric on the collection of all $m \times n$ matrices, see [4, 1].

The following is from [6, Definition 1].

Definition 1. Let C be an L-linear code. Let $\mathbf{c} \in C$. Then $\text{Rsupp}(\mathbf{c})$, the *rank support* of $\mathbf{c}$ is the K-linear row space of $M_B(\mathbf{c})$. So $\text{wt}_R(\mathbf{c})$ is the dimension of $\text{Rsupp}(\mathbf{c})$. Let D be an L-linear subcode of C. Then $\text{Rsupp}(D)$, the *rank support* of D is the K-linear space generated by the $\text{Rsupp}(\mathbf{d})$ for all $\mathbf{d} \in D$. Then $\text{wt}_R(D)$, the *rank support weight* of D is the dimension of $\text{Rsupp}(D)$.

Definition 2. Let C be an L-linear code. Then $d_{R,r}(C)$, the r-th *generalized rank weight* of the code C is the minimal rank support weight of a subcode D of C of dimension r.

The above is not the only proposed definition of the generalized rank weights. The first proposal of a definition of the r-th generalized rank weight was given by Kurihara-Matsumoto-Uyematsu [8, 9]. An alternative was given by Oggier-Sboui [10] and Ducoat [3]. Both definitions were motivated by applications.

3 Some codes related to C

With respect to the Hamming distance and a k-dimensional $\mathbb{F}_q$-linear code C, the support of C is defined by $\text{supp}(C) = \{j | c_j \neq 0 \text{ for some } \mathbf{c} \in C\}$. The subcode $C(J)$ is defined in [7] and [5, Definition 5.1] for a subset J of $\{1, \dots, n\}$ with complement J^c by:

$$C(J) = \{ \ \mathbf{c} \in C \mid \text{supp}(\mathbf{c}) \subseteq J^c \ \}.$$

Define $C(j) = C(\{j\})$ for $j \in \{1, \dots, n\}$. Let $J = \text{supp}(C)$. Then $C(j)$ has codimension one in C for all $j \in J$.

For the definition of $C(J)$ in the context of the rank metric we give the following analogous definition as given in [6, Definition 2].

Definition 3. Let L be a finite field extension of the field K. Let C be an L-linear code. For a K-linear subspace J of K^n we define:

$$C(J) = \{ \ \mathbf{c} \in C \mid \text{Rsupp}(\mathbf{c}) \subseteq J^{\perp} \ \}$$

From this definition it is clear that $C(J)$ is a K-linear subspace of C, but in fact it is also an L-linear subspace.

Lemma 4. *Let C be an L-linear code of length n and let J be a K-linear subspace of K^n. Then $\mathbf{c} \in C(J)$ if and only if $\mathbf{c} \cdot \mathbf{y} = 0$ for all $\mathbf{y} \in J$. Furthermore $C(J)$ is an L-linear subspace of C.*

Proposition 5. *Let $L = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$. Let C be an L-linear code.*
If $m \geq n$, then there exists a $\mathbf{c} \in C$ such that

$$\mathrm{Rsupp}(\mathbf{c}) = \mathrm{Rsupp}(C).$$

4 Galois closure and trace

Before we can give the various definitions of the generalized rank weights, we introduce the framework in which we study them.

Definition 6. Let L/K be a Galois extension. Let $C \subseteq L^n$ be an L-linear subspace. The *trace map* $\mathrm{Tr} : L^n \to K^n$ is the component-wise extension of the trace map $\mathrm{Tr} : L \to K$. The *restriction* of C is defined by $C|_K = C \cap K^n$. The *Galois closure* C^* of C is the smallest subspace of L^n that contains C and that is closed under the component-wise action of the Galois group of L/K. A subspace is called *Galois closed* if and only if it is equal to its own Galois closure.
If C is a K-linear subspace, then we define the *extension code* $C \otimes L$ as the subspace of L^n formed by taking all L-linear combinations of words of C.

Theorem 7. *Let $\mathbf{c} \in C$. Then the rows of the matrix $M(\mathbf{c})$ are elements of the trace code $\mathrm{Tr}(C)$ and*

$$\mathrm{Rsupp}(C) = \mathrm{Tr}(C)$$

.

Corollary 8. *Let D be a subcode of the L-linear code C. Then*

$$\mathrm{Rsupp}(D) = \mathrm{Tr}(D) \quad \textit{and thus}$$

$$d_{R,r}(C) = \min_{\substack{D \subseteq C \\ \dim(D) = r}} \mathrm{wt}_R(D) = \min_{\substack{D \subseteq C \\ \dim(D) = r}} \dim \mathrm{Tr}(C) = \min_{\substack{D \subseteq C \\ \dim(D) = r}} \dim D^*$$

5 Equivalent definitions

We will now discuss previous definitions of the generalized Hamming weights and to what extend they are consistent with Definition 2. The definition of Oggier-Sboui in [10] is, in our notation, as follows:

Definition 9. Consider the field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$. Let C be an $\mathbb{F}_{q^m}$-linear code and let $m \geq n$. Then the r-th generalized rank weight is defined as

$$\min_{\substack{D\subseteq C\\ \dim(D)=r}} \max_{\mathbf{d}\in D} \mathrm{wt}_R(\mathbf{d}).$$

Note that this definition is equivalent to Definition 2, since a subcode D contains a word of maximal rank weight by Proposition 5. Kurihara-Matsumoto-Uyematsu [8, 9] define the *relative generalized rank weights*, that induce the following definition of the generalized rank weights:

Definition 10. Consider the field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$. Let C be an $\mathbb{F}_{q^m}$-linear code. Then the r-th generalized rank weight is defined as

$$\min_{\substack{V\subseteq L^n, V=V^*\\ \dim(C\cap V)\geq r}} \dim V.$$

Both of Definitions 9 and 10 have an obvious extension to rank metric codes over the field extension L/K. Where possible, we will show the equivalence between the definitions in as much generality as possible.
Ducoat [3] proved the following for $m \geq n$:

$$\min_{\substack{D\subseteq C\\ \dim(D)=r}} \max_{\mathbf{d}\in D^*} \mathrm{wt}_R(\mathbf{d}) = \min_{\substack{V\subseteq L^n, V=V*\\ \dim(C\cap V)\geq r}} \dim V.$$

The left hand side is almost Definition 9, but with D^* instead of D in the maximum. The proof of the following theorem is largely inspired by Ducoat; note that it works more general over L instead of $\mathbb{F}_{q^m}$:

Theorem 11. *Let L be a Galois extension of K. Let C be an L-linear code. Then Definitions 10 and 2 give the same values, that is,*

$$\min_{\substack{V\subseteq L^n, V=V^*\\ \dim(C\cap V)\geq r}} \dim V = \min_{\substack{D\subseteq C\\ \dim D=r}} \dim D^*.$$

We now state the equivalence between Definitions 9 and the variation of 2 as used before.

Theorem 12. *Let L be a cyclic Galois extension of K of degree m. Let C be an L-linear code in L^n with $m \geq n$. Then*

$$\max_{\mathbf{d}\in D^*} \mathrm{rk}(M(\mathbf{d})) = \dim D^*$$

References

[1] D. Augot, P. Loidreau and G. Robert, *Rank metric and Gabidulin codes in characteristic zero*, IEEE ISIT-2013, International Syposium on Information Theory, pp. 509–513 (2013).

[2] D. Augot, *Generalization of Gabidulin codes over rational function fields*, MTNS-2014, 21st International Syposium on Mathematical Theory of Networks and Systems, arxiv:1412.6080v1.pdf, 2014.

[3] J. Ducoat, *Generalized rank weights: a duality statement*, arXiv:1306.3899v2, 2014.

[4] È.M. Gabidulin, *Theory of codes with maximum rank distance*, Problemy Peredachi Informatsii **21**, pp. 3–16 (1985).

[5] R.P.M.J. Jurrius and R. Pellikaan, *Codes, arrangements and matroids*, Series on Coding Theory and Cryptology **8**, World Scientific, Algebraic Geometry Modeling in Information Theory, E. Martínez-Moro (ed.), pp. 219–325 (2013).

[6] R.P.M.J. Jurrius and R. Pellikaan, *The extended and generalized rank weight enumerator*, Proc. ACA 2014, Applications of Computer Algebra, CACTC@ACA Computer Algebra in Coding Theory and Cryptography, Fordham University, New York, 2014.

[7] K.L. Katsman and M.A. Tsfasman, *Spectra of algebraic-geometric codes*, Problemy Peredachi Informatsii **23**, pp. 19–34 (1987).

[8] J. Kurihara, R. Matsumoto T. and Uyematsu, *New parameters of linear codes expressing security performance of universal secure network coding*, Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference, pp. 533–540 (2012).

[9] J. Kurihara, R. Matsumoto T. and Uyematsu, *Relative generalized rank weight of linear codes and its applications to network coding*, arXiv:1301.5482v1, 2013.

[10] F. Oggier, F. and A. Sboui, *On the existence of generalized rank weights*, IEEE ISIT-2012, International Syposium on Information Theory, pp. 406–410 (2012).

SBS: A Fast and Provably Secure Code-Based Stream Cipher

Extended Abstract — June 19, 2015

Pierre-Louis Cayrel[1], Mohammed Meziani[2], and Ousmane Ndiaye[3]

[1] Laboratoire Hubert Curien, UMR CNRS 5516,
Bâtiment F 18 rue du Benoît Lauras, 42000 Saint-Etienne
pierre.louis.cayrel@univ-st-etienne.fr
[2] CASED - Center for Advanced Security Research Darmstadt
Mornewegstrasse, 64293 Darmstadt, Germany
mohammed.meziani@cased.de
[3] Université Cheikh Anta Diop de Dakar, FST, DMI, LACGAA,
Senegal,
ousmane3.ndiaye@ucad.edu.sn

Abstract. We propose a new synchronous stream cipher, called SBS, based on iterating a set of Niederreiter's functions. Our proposal is characterized by a high software performance. Its speed is comparable to the AES encryption in counter mode. It runs at 7.8 cycles per byte. We have performed detailed security analysis, in particular, we prove that the security of SBS is reducible to the syndrome decoding problem. More precisely, we show that distinguishing the keystream generated by SBS is hard as solving an instance of the regular syndrome decoding problem.

Keywords: Stream ciphers, Provable security, Syndrome decoding.

1 Introduction

Roughly speaking, a stream cipher (or also pseudo-random generator) is a symmetric key algorithm that can be regarded as a "black-box" which produces sequence of bits that appears pseudo-random using a secret key (and a public vector, called a nonce). The term "pseudo-random" means that the generated sequence is computationally indistinguishable from a truly random sequence.

A number of efficient stream ciphers have been proposed in the literature, several of those were proven to be insecure as reported during the eSTREAM[4] project. Therefore, the main challenge is to design a stream cipher which has very fast implementations in software and hardware and which is provably secure, in the sense that recovering the secret key or producing a valid key stream is polynomial-time reducible to the solution of a hard cryptographic problem. As always, the first proposals in this direction were based on the hardness of well-known problems coming from number theory (e.g. factoring [13, 12], discrete logarithm [23], RSA problem [1]). However, this kind of system involves complex operations over big integers and is vulnerable to quantum attacks as demonstrated in [33].

Cryptographic schemes based on error-correcting code are among the most promising post-quantum candidates [10, 16, 9]. Their security relies on the problem that it is on average hard to decode generic random codes. In addition, they enjoy very interesting features. They are very fast, since they uses mostly very simple operations like shifts and XORs allowing a fast hardware and software implementations.

In code-based cryptography, Fischer and Stern [18] first came up with the idea of designing a pseudo-random generator, whose security is proven to rest on the hardness of the syndrome decoding problem [7]. However, their construction was inefficient because it needs enormous computational and memory requirements. The SYND stream cipher, proposed by Gaborit et al. [19], outperforms the Fischer-Stern's proposal in terms of storage space and performance. It uses quasi-cyclic (QC) random codes allowing for a decrease

[4] http://www.ecrytp.eu.org/stream

in the storage capacity and introduces the so-called regular encoder for speeding up the key stream generation. Their proposal is based on the hardness of decoding QC random codes [20, 6]. Recently, a new design, called 2SC, due to Meziani et. al [26], is proposed based on the same problem. It runs faster than previous construction, but needs much storage space.

Our contribution. The present paper proposes an efficient implementation of a provably secure code-based stream cipher which we call SBS. Its security is reducible to the hardness of the syndrome decoding problem. Moreover, this scheme is very efficient in terms of storage space, and outperforms all previous provably secure constructions. Its performance is comparable to AES according to the fastest implementation of AES.

Organization of the paper. The structure of this paper is distributed as follows. In Section 2, we present the concepts that are used throughout the text and basic facts about code-based cryptography. Then, we give a brief discussion of SYND [19] as related work in Section 3. In Section 4, we describe in detail our proposal, then perform detailed security analysis in Section 5. In Section 6, we address attacks and countermeasures based on the parameters choice. Section 7 presents experimental results and compares them to others schemes such as SYND [19], 2SC [26] or to their improved version detailed in [15]. Section 8 concludes the paper.

2 Preliminaries

The following briefly introduces the definitions and notations used in the present paper.

2.1 Notations

- $\star$ $|x|$ is the length in bits of a string x.
- $\star$ The Hamming weight of a string x is the number of its non-null coordinates and denoted by $\texttt{wt}(x)$.
- $\star$ $x^\top$ is the transpose of a string x.
- $\star$ $x\|y$ (resp. $X\|Y$) represents the concatenation of two strings x and y (resp. of two matrices X and Y)
- $\star$ $x \oplus y$ denotes the bitwise XOR of two strings x and y, having the same size.
- $\star$ For a finite set S, we denote by $x \overset{\$}{\leftarrow} S$ the experiment of uniformly at random choosing an element x from S and assigning it to x.
- $\star$ We write $\mathcal{M}_{\ell,\eta}$ to indicate the set all binary random matrices of size $\ell \times \eta$.
  The notation $\mathsf{H} \overset{\$}{\leftarrow} \mathcal{M}_{\ell,\eta}$ is the random process of uniformly selecting a matrix H from $\mathcal{M}_{\ell,\eta}$.
- $\star$ We denote by $[N]$ the set $\{0, \cdots, N-1\}$.
- $\star$ If x is a bit string, then $\texttt{Int}(x)$ denotes the integer corresponding to x in big-endian format.
- $\star$ We write $\mathcal{W}_{\eta,\omega}$ for the set of all strings of length η and weight ω.
- $\star$ For two bit strings a and b having the same length, the binary value $\langle a, b\rangle = \sum_i a_i b_i \mod 2$ defines their dot inner product.

2.2 Basics on linear codes

An (η, κ)-binary linear code $\mathcal{C}$ is a subspace of $\mathbb{F}_2^\eta$ of *dimension* κ. An elements of $\mathbb{F}_2^\eta$ is called *word* and an element of $\mathcal{C}$ is a *codeword.* We call η the *length*, κ the *dimension* of the code. A *parity-check* matrix H of a code $\mathcal{C}$ is an $(\eta-\kappa)\times\eta$ matrix whose rows form a basis of the orthogonal complement of $\mathcal{C}$, i.e. $\mathcal{C} = \{x \in \mathbb{F}_2^\eta \ : \ \mathsf{H}\cdot x^\top = \mathbf{0}\}$.
A code $\mathcal{C}$ is called *cyclic* if it is invariant under a right cyclic shift, i.e. $(x_1, x_2, \ldots, x_\eta) \in \mathcal{C}$ if and only if $(x_\eta, x_1, \ldots, x_{\eta-1}) \in \mathcal{C}$. In this case, a parity check matrix H of a cyclic code is only described by its first row. Such matrix is also called *circulant.* A block matrix H is called *quasi-cyclic* if it is composed of a number of cyclic sub-matrices.
A *syndrome* of x is a string $s \in \mathbb{F}_2^{\eta-\kappa}$ such that $s = \mathsf{H}\cdot x^\top$, where H is an $(\eta-\kappa)\times\eta$ parity check matrix.
A word x of length η and weight ω is called *regular* if it consists of ω blocks, each having length $\lfloor\frac{\eta}{\omega}\rfloor$ and containing exactly one "1". We denote the set of those words by $\mathcal{R}_{\eta,\omega}$.

The (binary) *Gilbert-Varshamov* (GV) bound is the smallest positive integer d satisfying $\sum_{j=0}^{d} \binom{\eta}{j} \geq 2^{\eta-\kappa}$. For large values of η, this inequality becomes $\binom{\eta}{d} \geq 2^{\eta-\kappa}$. If the weight ω is smaller than this bound, then there is at most one solution of the following problems. Otherwise, there can be several solutions.

2.3 Hard problems in codes

The security of most constructions in code-based cryptography is related to (conjuctured) intractability of following computational problems.

The Syndrome Decoding Problem (SDP). This problem underlies the security of most of the code-based cryptographic primitives (see [10, 32, 14] for more details). In this problem we are given a binary matrix $\mathsf{H} \in \mathcal{M}_{\ell,\eta}$, an element $s \in \mathbb{F}_2^\ell$, and a non-negative integer $\omega < \ell$, our task is to find an element $x \in \mathcal{W}_{\eta,\omega}$ such that $s = \mathsf{H} \cdot x^\top$. The decisional version of this problem was originally called *Coset Weights* and proved $\mathcal{NP}$-complete in [7] for generic random codes. No known polynomial-time (PT) algorithms for solving the SDP has been found up to date. All published algorithms for solving the SDP are probabilistic and have an exponential running time in code length η (See [25] for the best known attack).

A special case of this problem is called the regular syndrome decoding, where solutions (if there exist) belonging to the set of all regular words. This problem was also shown to be $\mathcal{NP}$-complete by Augot et al. [3], and is as difficult as the SDP, since there is no known algorithm that can do significantly better than the best algorithm [25] proposed against the SDP.

3 Related work

The SYND stream cipher. As mentioned in the introduction, Gaborit et. al [19] proposed an improved version of the Fischer-Stern's pseudo-random number generator [18] by making two major modifications: introducing the quasi-cyclic codes considerably decreases the storage requirements space, and working with regular words instead of classical words significantly improves the performance of the system. In what follows, we briefly describe the main ingredients in the SYND stream cipher without going into details.

Let η, ω, and ℓ be three positive integers such that the ratio $\frac{\eta}{\omega}$ is a power of two and $\ell = \omega \log_2(\frac{\eta}{\omega})$. SYND essentially consists of two steps: initialization phase and key stream generation step. Both use two ℓ-to-ℓ mappings f_1 and f_2 as building block. These mappings are defined by

$$f_1(x) = A \cdot \theta(x)^\top; \quad f_2(x) = B \cdot \theta(x)^\top, \quad \forall x \in \mathbb{F}_2^\ell,$$

where A and B are random binary matrices describing the same binary quasi-cyclic (QC) code of length η, correcting up to ω errors, and $x \mapsto \theta(x)$ is an encoding function transforming ℓ-bit strings to regular words. We omit here how this function works, and we refer, for example, to [3, 2]. Furthermore, we only describe the key stream generation phase without explaining how initial states are generated. Given an initial state e_0 generated by using a secret key K and an initial value IV, the key stream formed by a number of block z_i is produced as follows: apply f_1 on the current state e_i to get the next state $e_{i+1} = f_1(e_i)$ (updating the current state), and then compute the output block z_i by $z_i = f_2(e_i)$. As shown in [19], this process can be modeled by using one function f, which is a concatenation of f_1 with f_2, i.e., $f(x) = f_1(x) \| f_2(x)$, for $x \in \mathbb{F}_2^\ell$.

As we can straightforward see, in order to produce an output block, the mapping f_2 first has to wait for evaluating the mapping f_1 at some state every time. This makes the whole process not full parallelizable using the state-of-the art programming techniques. Our main motivation in this work is how to design a SYND-like stream cipher that can be completely implemented in parallel manner, and hence has better computational features than the SYND stream cipher, and can be proved to be provably secure. We note that SYND's authors did not give any detail about the security reduction of their proposal, but they only claimed that the security reduction can be deduced from the QUAD stream cipher [5] and the Fischer-Stern PRNG [18].

4 The SBS Cipher

In this section we provide a detailed description of the SBS cipher and its basic ingredients. The letters in its name stand for "Syndrome Based Stream".

The building blocks of the SBS cipher are two code-based one-to-one transformations ϕ_1 and ϕ_2 that accept as input a bit string and return a bit string of the same size as the input. The SBS is a synchronous stream cipher and parameterized by a set of positive integers (η, ℓ, ω) satisfying $\ell = \omega \log_2(\frac{\eta}{\omega})$, where $\omega < \ell < \eta$. This set determines the size of an internal state, the key length, and the size of an initial vector (IV). For security reasons, IV of the same length as the secret key are used, both have $\lfloor \frac{\ell}{2} \rfloor$ bits. The SBS is composed of two major blocks, `Initializer`, and `Generator`, both implicitly use two transformations ϕ_1 and ϕ_2 that we will describe later.

`Initializer:` $\mathtt{F} : \mathbb{F}_2^{|K|} \times \mathbb{F}_2^{|IV|} \to \mathbb{F}_2^{\ell} \times \mathbb{F}_2^{\ell}$.
It takes as input the initialization vector (IV) and the key (K) in order to calculate the initial state $s_0 = (x_0, y_0)$, according the following steps:

$$\alpha = K \| IV \tag{1}$$

$$\beta = \alpha \oplus \phi_1(\alpha) \tag{2}$$

$$\gamma = \alpha \oplus \phi_2(\alpha) \tag{3}$$

$$s_0 = (x_0, y_0) = \mathtt{F}(\alpha) = (\beta \oplus \phi_2(\beta), \gamma \oplus \phi_1(\gamma)) \tag{4}$$

During the initialization stage no output bits are returned, only after s_0 is produced, key stream generation is allowed to take place.
`Generator:` $\mathtt{G} : \mathbb{F}_2^{\ell} \times \mathbb{F}_2^{\ell} \to \mathbb{F}_2^{\ell} \times \mathbb{F}_2^{\ell}$.
It takes as input the initial state s_0 generated by $\mathtt{F}$, and produces a 2ℓ-bit string $(u_i, v_i), i \geq 1$ in each round. A simple block diagram of this generator is shown in Figure 1. The creation of $\{s_{i+1}\}_{i \geq 0}$ works as follows. Starting with $s_i = (x_i, y_i)$, the generator $\mathtt{G}$ outputs (u_i, v_i) and updates s_i (or computes the subsequent state $s_{i+1} = (x_{i+1}, y_{i+1})$) by executing the following computations (in parallel):

1. $x_{i+1} \leftarrow \phi_1(x_i)$ and $y_{i+1} \leftarrow \phi_2(y_i)$
2. $u_i \leftarrow \phi_1(y_i)$ and $v_i \leftarrow \phi_2(x_i)$

During this process, only u_i and v_i are returned as output and visible to an adversary.

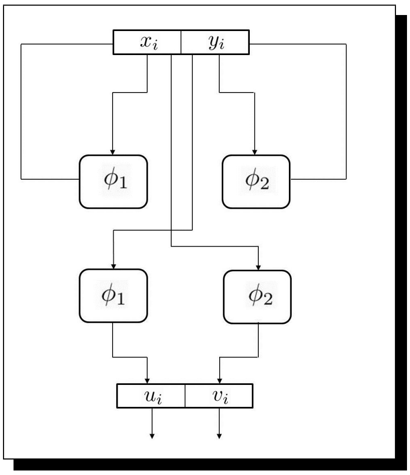


Fig. 1. Block diagram of SBS generator

Note that ϕ_1 and ϕ_2 are called at the same time with different inputs, so that the implementation of $\mathtt{G}$ can be fitted to the parallelism of modern CPUs. The whole process of the key stream generation of SBS can be described by a single function $\mathtt{h}$ that takes as input a 2ℓ-bit string and expands it into a 4ℓ-bit string in each iteration. This function is defined as follows:

$$\mathtt{h}(x, y) := \mathtt{f}(x, y)\|\mathtt{g}(x, y) \in \mathbb{F}_2^{4\ell}, \tag{5}$$

where $(x, y) \to \mathtt{f}(x, y) := (\phi_1(x), \phi_2(y)))$ is an update function, that refreshes the current state (x, y), while $(x, y) \to \mathtt{g}(x, y) := (\phi_1(y), \phi_2(x)$ is an output function producing an 2ℓ-bit string which form the key stream bit of SBS.

Now, we want to describe how the transformations ϕ_1 and ϕ_2 in the SBS cipher are implemented. Let A and B be two randomly chosen binary matrices of the same size $\ell \times \eta$. Let $(x_1, \cdots, x_\omega)$ be the decomposition of $x \in \mathbb{F}_2^\ell$, i.e., x consists of ω binary pieces, each of them has $\log_2(\frac{\eta}{\omega})$ bits. For simplicity, we set $\sigma := \log_2(\frac{\eta}{\omega})$. By doing so, we obtain 2^σ distinct decimal values for each x_i, ranging from 0 to $2^\sigma - 1$. Next, since $\eta = \omega 2^\sigma$, then each decimal value of x_i will be associated with a certain column of the matrix A and B. By combining all corresponding columns together, we get an ℓ-bit string, which is the output of the transformation. In SBS we use the bitwise-XOR operator as combiner. A block diagram of ϕ_1 (or ϕ_2) is depicted in Figure 2.

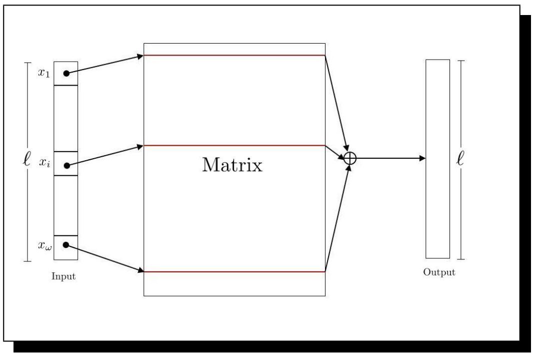


Fig. 2. Block structure of the transformations used in SBS

5 Security reduction of SBS

This section deals with the security of SBS cipher. Before we go into more details, we introduce the assumptions, that we use to prove the security of the SBS cipher. These assumptions are the basis for proving the security of Fischer-Stern's pseudo-random number generator [18].

The first assumption ($\mathtt{A1}$), called *indistinguishabiliy*, reads as follows:

"It is computationally infeasible to distinguish two matrices A and B from uniform random ones having the same dimensions".

Here we use the same idea in QUAD [5] for the security reduction to syndrome decoding problem. This security reduction permits to say: breaking the SBS scheme means to break the syndrome decoding problem which is $\mathcal{NP}$-complete.

Lemma 1. *Let $L = 2\lambda\ell$ be the number of keystream bits produced by the scheme in time λT_S using λ iterations. Suppose there exists an algorithm $\mathcal{A}$ that distinguishes the L-bit keystream sequence associated with two known randomly chosen $\ell * \eta$ matrices A and B and an unknown randomly chosen initial internal state (x, y) of weight at most 2ω of $\{0, 1\}^\eta$ from a random L-bit sequence in time T with advantage ϵ. Then there exists an algorithm $\mathcal{B}$, which given the image $\mathsf{H} \cdot z^\top$ of a randomly chosen regular word z of weight ω of $\{0, 1\}^\eta$ by a randomly chosen $\ell \times \eta$ matrix H permits to recover z in time $T = T + \lambda T_S$ with advantage at least $\frac{\epsilon}{\lambda}$.*

Proof. One can see $\mathsf{H} \cdot z^\top = \begin{pmatrix} \mathsf{H} & 0 \\ 0 & \mathsf{H} \end{pmatrix} \begin{pmatrix} z^\top \\ 0 \end{pmatrix}$ to be the output of the initial state $(z, 0)$.
We assume that $\mathsf{H} \cdot z^\top = g(z, 0)$, with random matrices $A = B := \mathsf{H}$ and for each round $0 \leq i \leq \lambda - 1$ the outputstream is $g(f^i(z, 0))$. For the remainder, we follow the QUAD reduction.

■

The second assumption (`A2`), called *Syndrome Decoding*, states the following:
"The collection of functions $\{F_\mathsf{M}\}_{\mathsf{M} \in \mathcal{M}_{\ell,\eta}}$ defined over the set $\mathcal{W}_{\eta,\omega}$ as $F_\mathsf{M}(x) = \mathsf{M} \cdot x^\top$ is one-way".

The third assumption (`A3`), called *Regular Syndrome Decoding*, is a particular case of `A2` and reads as follows:
"The collection of functions $\{F_\mathsf{M}\}_{\mathsf{M} \in \mathcal{M}_{\ell,\eta}}$ defined over the set $\mathcal{R}_{\eta,\omega}$ as $F_\mathsf{M}(x) = \mathsf{M} \cdot x^\top$ is one-way".
For `A1` and `A3` see [3]. Now we need the following Lemmas.

Lemma 2. *If the assumption `A3` holds, then the transformation ϕ_1 (and ϕ_2) implemented in SBS is one-way.*

Proof. To prove this lemma, it is sufficient to show that ϕ_1 (and ϕ_2) can be transformed into a function selected from the collection defined in `A2`. Choose $\mathsf{A} \overset{\$}{\leftarrow} \mathcal{M}_{\ell,\eta}$ such that $\ell = \omega \cdot \sigma$, where $\omega < \ell < \eta$, $\sigma = \log_2(\frac{\eta}{\omega})$, and $\eta = \omega 2^\sigma$. Then the matrix A can be partitioned into ω sub-matrices consisting of 2^σ columns and ℓ lines, i.e., $\mathsf{A} = \mathsf{A}_1 | \ldots | \mathsf{A}_\omega$. Let $(x_1, \cdots, x_\omega)$ be the input of ϕ_1, where $|x_i| = \sigma$. Consequently, each x_i can be uniquely associated with a column number $d_i \in [2^\sigma]$, of the sub-matrix A_i using the big-endian form. These column positions $(d_i)_{i=1}^{\omega}$ form a regular word $z = (z_1, \cdots, z_\eta)$ of length η and weight ω such that $z_j = 1$ if $j = d_i$ and $z_j = 0$ otherwise. By doing so, one can easily check that $\phi_1(x) = \mathsf{A} \cdot z^\top$.

■

Lemma 3. *If the assumption `A2` holds, then the transformations `f` and `g` are both one-way.*

Proof. This straightforward results from [21, 35], that state that for every collection of one-way functions $\mathcal{F} = \{f_k\}_{k \in S}$, where S is a finite set, the collection $\mathcal{F}_n = \{f_{i_1,\cdots,i_n}\}_{i_1,\cdots,i_n \in S^n}$, whose elements are defined as $f_{i_1,\cdots,i_n}(x_1, \cdots, x_n) = (f_{i_1}(x_1), \cdots, f_{i_n}(x_n))$ is also one-way. In addition, this is even true when having a single mapping (i.e., when $i_1 = \cdots = i_n$). In our setting, we have $S = \{1, 2\}$.

■

In order to prove that SBS is a pseudo-random generator, we will prove that the sequence pair (u_i, v_i) is pseudo-random, meaning that it is indistinguishable from an 2ℓ-bit random string. We will demonstrate this by induction. We need the following definition:

Let `F` be a one-way function. A hardcore bit $\mathtt{b} : \{0,1\}^* \to \{0,1\}$ for `F` is a polynomial-time computable function such that if for all PPT adversary $\mathcal{A}$ there exists one negligible function ϵ, such that

$$\Pr[\mathcal{A}(\mathtt{F}(x)) = \mathtt{b}(x)] \leq \frac{1}{2} + \epsilon(n), \quad \forall n$$

where the probability is over x chosen randomly and the coin tosses of $\mathcal{A}$. Related to this definition, Goldreich and Levin proved the following theorem, which can be informally stated as follows: for any one-way function, the dot product of its argument and a randomly chosen bit string is a hardcore bit (or hardcore predicate).

Theorem 1. *(Goldreich-Levin theorem) Let $F : \{0,1\}^* \to \{0,1\}^*$ be a one-way function. For every PPT algorithm $\mathcal{A}$, for all polynomials p and all but finitely many n's,*

$$\Pr[\mathcal{A}(F(x), \nu) = \langle x, \nu \rangle] \leq \frac{1}{2} + \frac{1}{p(n)}$$

where the probability is taken over x uniformly chosen x and ν.

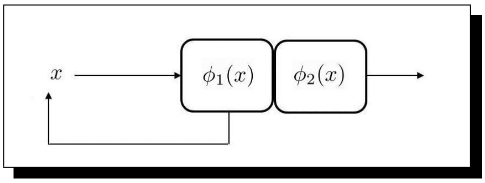


Fig. 3. Illustration of G_1

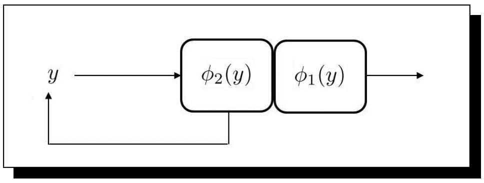


Fig. 4. Illustration of G_2

Theorem 2. *Let* R *and* L *be two functions defined over* $\mathbb{F}_2^\ell$ *by*

$$\mathsf{R} = \phi_1(x)\|\phi_2(x) \quad \textit{and} \quad \mathsf{L}(y) = \phi_2(y)\|\phi_1(y)$$

Related to R *and* L*, we define two* 2ℓ*-bit strings generator* $\mathsf{G_R}$ *and* $\mathsf{G_L}$ *depicted in Figure 3 and Figure 4, respectively. The function* ϕ_1 *(resp.* ϕ_2*) is the update (resp. output) function of* $\mathsf{G_R}$ *contrary to* $\mathsf{G_L}$*. If the assumptions* `A1` *and* `A3` *hold, then* $\mathsf{G_R}$ *and* $\mathsf{G_L}$ *are both pseudo-random generators.*

Proof. It is sufficient to prove this statement for $\mathsf{G_R}$, since they are similar. The proof is an adaptation of that given in [18]. Note that R and is L are both expansion functions with expansion factor 2.
Lemma 2 shows that the function ϕ_1 (resp. ϕ_2) can be rewritten as $\phi_1(x) = \mathsf{A} \cdot z^\top$ (resp. $\phi_2(x) = \mathsf{B} \cdot z^\top$), where z is a regular word that corresponds to the input x. Hence, if we vertically stack A and B, we obtain a new $2\ell \times \eta$ matrix M given by

$$\mathsf{M} = \begin{pmatrix} \mathsf{A} \\ \mathsf{B} \end{pmatrix}$$

This matrix satisfies the assumption `A1`. We can then write $\mathsf{R}(x) = \mathsf{M} \cdot z^\top$. So, it would be sufficient to prove that the output of $\mathsf{M} \cdot z^\top$ is pseudo-random. Now, we show by contradiction that the output of R is pseudo-random. Suppose the opposite. Then there is a distinguisher Ψ that can make a distinction between this output and an 2ℓ-bit random sequence u. This distinguisher accepts as input an $2\ell \times \eta$ binary random matrix M and a random $u \in \{0,1\}^{2\ell}$ as a candidate being equal to $\mathsf{M} \cdot z^\top$ for some unknown regular word z. If $\mathsf{M} \cdot z^\top = u$, Ψ outputs 1 with probability above $\frac{1}{2} + \frac{1}{p(\eta)}$, for every polynomial $p(n)$. Otherwise, when u is chosen uniformly from $\{0,1\}^{2\ell}$, Ψ outputs 1 with probability at most $\frac{1}{2}$. More precisely, the behavior of Ψ is the following:

$$\begin{cases} \Pr[\Psi(\mathsf{M}, u) = 1] \geq \frac{1}{2} + \frac{1}{p(\eta)}, & \text{if } u = \mathsf{M} \cdot z^\top, \text{ for some regular word } z \\ \Pr[\Psi(\mathsf{M}, u) = 1] < \frac{1}{2}, & \text{if } u \text{ is taken uniformly from } \{0,1\}^{2\ell} \end{cases}$$

Our next step is to construct an algorithm Θ which calls Ψ as a subroutine, in order to predict the dot product of an unknown regular word z and a random chosen η-bit sequence v (i.e., $\langle z, v\rangle$) with probability at least $\frac{1}{2} + \frac{1}{2p(\eta)}$. To achieve this, we write $v = (v_1, \cdots, v_\eta)$ and define π to be the number of the positions j such that $z_j = v_j = 1$, i.e. the size of the intersection $z \cap v$. Let ϵ be its parity, i.e. the inner product $\langle z, v\rangle$. By doing so, on inputs $\mathsf{M} \cdot z^\top$ and v, the algorithm Θ will perform the following:

- Choose a random $\epsilon' \in \{0,1\}$ as candidate to ϵ
- Choose randomly $\delta \in \{0,1\}^{2\ell}$
- Construct a new $2\ell \times \eta$ binary matrix $\widehat{\mathsf{M}} = (\widehat{a}_1, \cdots, \widehat{a}_\eta)$ such that for every $j \in \{1, \cdots, \eta\}$ it holds

$$\widehat{a}_j = \begin{cases} a_j + \delta & \text{if } v_j = 1, \\ a_j & \text{if } v_j = 0 \end{cases}$$

  where $(a_1, \cdots, a_\eta)$ is the decomposition of M, that means $\widehat{\mathsf{M}} = M + \delta^\top \cdot v$
- Supply the distinguisher Ψ with $\widehat{\mathsf{M}}$ and $\widehat{\mathsf{M}} \cdot z^\top = \mathsf{M} \cdot z^\top + \epsilon' \cdot \delta^\top$
- If Ψ outputs 1, then output $\epsilon' = \epsilon$. Otherwise, returns the opposite of ϵ'.

Let us now show that Θ predicts the dot product $\langle z, v\rangle$ with probability above $\frac{1}{2} + \frac{1}{2p(\eta)}$.
There are to distinct cases to treat:

(1) $\mathtt{C}_1 := \{\epsilon$ guessed correctly$\}$. Then the predicted value for $\langle z, v\rangle$ is correct if the distinguisher outputs 1. But the distribution seen by the distinguisher on $(\widehat{\mathsf{M}}, \mathsf{M} \cdot z^\top + \epsilon' \cdot \delta^\top)$ is similar to the distribution on input $(\mathsf{M}, \mathsf{M} \cdot z^\top)$. By construction, this occurs with probability at least $\frac{1}{2} + \frac{1}{p(\eta)}$.
(2) $\mathtt{C}_2 := \{\epsilon$ not guessed correctly$\}$. The distinguisher receives uniformly distributed inputs because of the randomness of δ and therefore outputs 1 with probability $\frac{1}{2}$.

Seeing that $\Pr[\mathtt{C}_1] = \Pr[\mathtt{C}_2] = \frac{1}{2}$, we can clearly conclude that the entire success probability of predicting the dot product $\langle z, v\rangle$ is at least $\frac{1}{2} + \frac{1}{2p(\eta)}$. This leads to a contradiction with the Goldreich-Levin Theorem [22] due to assumption A3. As consequence, the function R (and also L) is pseudo-random.

■

Now we are ready to present the main result concerning the pseudo-randomness of the SBS stream cipher. The proof is inductive over the iteration number and involves Theorem 2.

Theorem 3. *Let (x_0, y_0) be a random initial state. If we choose parameters (η, ℓ, ω) such that assumptions A1 and A3 are met, then the SBS cipher is a pseudo-random generator.*

Proof. To this end, we will show that the sequences u_i and v_i are pseudorandom. We will prove this by induction over i.

- Base case: $i = 1$. From Theorem 2 we conclude that $\mathsf{R}(x_0) = \phi_1(x_0)\|\phi_2(x_0)$ and $\mathsf{L}(y_0) = \phi_2(y_0)\|\phi_1(y_0)$ are both 2ℓ-bit pseudo-random sequence. This implies also $u_0 = \phi_1(y_0)$ and $v_0 = \phi_2(x_0)$ are pseudo-random sequence. The same argument holds for $x_1 = \phi_1(x_0)$ and $y_1 = \phi_2(y_0)$.
- Induction step: Assume that u_j and v_j (and also x_j and y_j) are pseudo-random sequence for some positive integer j (the induction hypothesis). We will show that u_{j+1} and v_{j+1} are also pseudo-random sequences. We have the following relations:

$$\begin{cases} u_{i+1} = \phi_1(y_{i+1}), & y_{j+1} = \phi_2(y_j) \\ v_{i+1} = \phi_2(x_{i+1}), & x_{j+1} = \phi_1(x_j) \end{cases}$$

  By the induction hypothesis, the sequences $\mathsf{R}(x_j) = \phi_1(x_j)\|\phi_2(x_j)$ and $\mathsf{L}(y_j) = \phi_2(y_j)\|\phi_1(y_j)$ are pseudo-random. That means, $\phi_1(x_j) = x_{j+1}$ and $\phi_2(y_j) = y_{j+1}$ are pseudo-random and applying Theorem 2 on these sequences completes the inductive step and therefore the SBS cipher is a pseudo-random number generator.

■

6 Best known attacks against SBS

In this section, we present the best known generic algorithms for attacking SBS and verify whether they are applicable. We only focus on the hardness of inverting the underlying functions ϕ_1 and ϕ_2 involved in the initialization and key stream generation procedure, as they constitute the major components of SBS design. The inversion of ϕ_1 and ϕ_2 obviously allows for a successful key and state recovery. The complexity estimate of an attack Z against an instance of SBS with parameters (η, ω, ℓ) will be denoted by $\mathtt{CE}_{\mathtt{Z}}(\eta, \omega, \ell)$. This complexity is defined as the number of binary operations required to invert one of the functions ϕ_1 (or ϕ_2). In our estimates, the parameters set (η, ω, ℓ) is chosen as follows: $\ell = \omega\sigma$ with $\sigma = \log_2\left(\frac{\eta}{\omega}\right)$.

There basically exists three different potential algorithms: Information Set Decoding (ISD), Linearisation Attacks (LA) and Generalized Birthday Attacks (GBA). In our analysis, we will omit the details of the description of each algorithm and instead give a lower-bound estimate of its complexity. The reader can refer to the cited papers for further details.

Information Set Decoding (ISD). It is a probabilistic algorithm designed for decoding any linear code. Its first variant, introduced by Prange [30], has been updated and refined many times over the years leading to the best variant, recently developed by May et al. [25]. The basic idea behind this algorithm is to find a subset, called information set, of κ error-free positions amongst the η positions of each codeword, where κ and η are the length and the dimension of the underlying code. In each trial Gauss-elimination on the parity check matrix of dimension $\ell \times \eta$ is performed for testing the validity of this set, so that the complexity $\mathtt{CE}_{\mathtt{ISD}}(\eta, \omega, \ell)$ of this algorithm can be estimated by $\frac{\mathtt{GE}(\ell)}{\mathtt{PR}(\eta,\ell,\omega)}$. The quantity $\mathtt{GE}(\ell)$ expresses the complexity of Gauss-Elimination, while $\mathtt{PR}(\eta, \ell, \omega)$ is the probability to find a valid information set. In [3], a lower bound of the complexity of solving an instance of the RSDP (the cost of inverting ϕ_1) is presented and estimated by $(\omega\sigma)^3 \cdot \left(\frac{2^\sigma}{\sigma}\right)^\omega$. In this work, we use the lower bound of the best ISD algorithm presented in [25] to estimate the security of SBS against ISD attacks.

Linearization Attacks (LA). This kind of attacks belongs to linear cryptanalysis which is probably one of the most powerful tools available for attacking symmetric cryptosystems. In a nutshell, a linearization attack consists in constructing a linear expression that can be easily solved by the use of the techniques of linear algebra. Against our proposal we have identified two possible linearization algorithms: Saarinen's attack [31] and Bellare-Micciancio's algorithm (BM) [4]. The first attack has been designed for attacking the FSB hash family [3] and briefly consists in reducing the problem of finding collisions or preimages to that of solving system of linear equations. When $\ell \leq 2\omega$, its complexity only amounts to $0.29\ell^3$, where 0.29 is an approximation of the probability that a square random matrix is non-singular. On the contrary, when $\omega \leq \lambda$, for some positive integer this complexity becomes $\frac{2^\ell}{(\lambda+1)^\omega}$. In particular, for $\lambda = 2\mu$, Berstein et al. [11] have recently revised this complexity to $\frac{2^\ell}{(\mu+1)^{2\omega}}$. The second algorithm aims at inverting the so-called XHASH function by finding a linear relation between ω columns of length ℓ bits. This allows to build a system having $\omega + \ell$ equations with 2ℓ unknowns, which is straightforward to solve when $\omega = \ell + 1$. More generally, the complexity of inverting the mentioned function requires at least $2^{\ell-\omega}$ binary operations (see [4, Appendix A, Lemma A.1] for more details).

Generalized Birthday Attacks (GBA). This class of attacks attempt to solve the following, so-called k-sum problem: given k random lists $L_1, L_2, \ldots, L_k$ of ℓ-bit strings selected uniformly and independently at random, find $x_1 \in L_1, x_2 \in L_2, \ldots, x_k \in L_k$ such that $\oplus_{i=1}^k x_i = 0$. For $k = 2$, a solution can be found in time $2^{\frac{r}{2}}$ using the standard birthday paradox. For $k > 2$ Wagner's algorithm [34] and its extended variants [3, 8, 28, 17] can be applied. When $k = 2^{j-1}$ and $|L_i| > 2^{\frac{\ell}{j}}$, Wagner's algorithm can find at least one solution in time $2^{\frac{r}{j}}$.

The main idea behind a GBA algorithm is depicted Fig. 5. We consider the case $k = 4$. Let $L_1, \ldots, L_4$ be four lists, each of length $2^{\frac{\ell}{3}}$. The algorithm proceeds in two iterations. In the first iteration, we build two new lists $L_{1,2}$ and $L_{3,4}$. The list $L_{1,2}$ contains all sums $x_1 \oplus x_2$ with $x_1 \in L_1$ and $x_2 \in L_2$ such that the first $\frac{\ell}{3}$ bits of the sum are zero. Similarly, $L_{3,4}$ contains all sums $x_3 \oplus x_4$ with $x_3 \in L_3$ and $x_4 \in L_4$ such that the first $\frac{\ell}{3}$ bits of the sum are zero. So the expected length of $L_{1,2}$ is equal to $2^{-\frac{\ell}{3}} \cdot |L_1| \cdot |L_2| = 2^{\frac{\ell}{3}}$. Similarly, the expected length of $L_{3,4}$ is also $2^{\frac{\ell}{3}}$. In the second iteration of the algorithm, we construct a new list L'_1 containing all pairs $(x'_1, x'_2) \in L_{1,2} \times L_{3,4}$ such that the first $\frac{\ell}{3}$ bits of the sum $x'_1 \oplus x'_2$ are zero. Then the probability that $x'_1 \oplus x'_2$ equals zero is $2^{-\frac{2\ell}{3}}$. Therefore, the expected number of matching sums is $2^{-\frac{2\ell}{3}} \cdot |L_{1,2}| \cdot |L_{3,4}| = 1$. So we expected to find a solution. This idea can be generalized for $k = 2^{j-1}$ by repeating the same procedure $j-2$ times. In each iteration a, we construct lists, each containing $2^{\frac{\ell}{j}}$ elements that are zero on their first $\frac{a\ell}{j}$ bits, until obtaining, on average, one ℓ-bit element with all entries equal to 0.

For selecting secure parameters of the SBS stream cipher against GBA attacks, we use the GBA algorithm from [17]. This algorithm attempts to find a set of indices $I = \{1, 2, \ldots, 2^\gamma\}$ satisfying $\oplus_{i \in I} H_i = 0$, where H_i are columns of the matrix H. As shown in [17], the algorithm is applicable when $\binom{2^b w}{2^{(1-\gamma)w}} \geq 2^{bw+\gamma(\gamma-1)}$. Under this condition, the cost of solving an instance RSD problem with parameters (n, r, w) is at least approximated by $\left(\frac{wb}{\gamma} - 1\right) 2^{\frac{wb}{\gamma}-1}$.

Note that [29] shows that the time and memory efficiency of GBA attacks can be improved, but only by a small factor. In Section 7, we take this improvement into account when proposing parameters for XSYND [27].

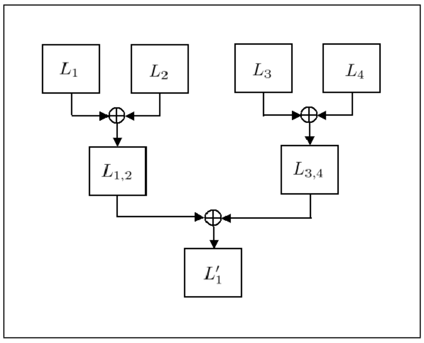


Fig. 5. The GBA idea for $k = 4$.

Remark. The equations defining u_i and v_i can be expressed as function in y_0 and x_0, respectively. Actually, it is easy to check that

$$\begin{cases} x_i = \phi_1^{(i)}(x_0), \quad y_i = \phi_2^{(i)}(y_0) \\ u_i = \phi_1(\phi_2^{(i-1)}(y_0)), \quad v_i = \phi_2(\phi_1^{(i-1)}(x_0)) \end{cases}$$

With this setting, if x_0 (resp. y_0) is fixed point of ϕ_1 (resp. ϕ_2), then the SBS will produce identical key stream in each iteration and therefore the attacker can correctly guess the subsequent key stream generated by SBS. Fortunately, this event will occur with negligible probability. In order to prove this statement, we need the following lemma.

Lemma 4. *Let $0 < \theta < 1$, and $Z_1, Z_2, \cdots, Z_t$ be independent random variables over $\{0,1\}$ such that $\Pr[Z_i = 1] = \theta$, $\forall i \in \{1, \cdots, t\}$. Then,* $\Pr\left[\sum_{i=1}^{t} Z_i \equiv 1 \mod 2\right] = \frac{1}{2} - \frac{(1-2\theta)^t}{2}$.

Proof. It is straightforward to show (per induction) that

$$\sum_{i=1}^{t} Z_i \equiv 0 \mod 2 \;\Leftrightarrow\; \prod_{i=1}^{t}(-1)^{Z_i} = 1 \tag{6}$$

From that it follows :

$$\Pr\left[\sum_{i=1}^{t} Z_i \equiv 0 \mod 2\right] = \Pr\left[\prod_{i=1}^{t}(-1)^{Z_i} = 1\right]. \tag{7}$$

Furthermore, if W is a random variable taking values from $\{-1,1\}$ then its expected value $E(W)$ is equal

$$E(W) = \Pr[W = 1] - \Pr[W = -1] = 1 - 2\Pr[W = -1]. \tag{8}$$

If we set $W = \prod_{i=1}^{t}(-1)^{Z_i}$, then using the fact that $Z_1, Z_2, \cdots, Z_t$ are independent, we obtain

$$E(W) = \prod_{i=1}^{t} E\left((-1)^{Z_i}\right) = \prod_{i=1}^{t}(1 - 2\theta) = (1 - 2\theta)^t. \tag{9}$$

Combining equations (8) and (9), we get the claimed equation

$$\Pr\left[\sum_{i=1}^{t} Z_i \equiv 1 \mod 2\right] = P[W = -1] = \Pr\left[\prod_{i=1}^{t}(-1)^{Z_i} = -1\right] = \frac{1}{2} - \frac{(1-2\theta)^t}{2}. \tag{10}$$

■

Now we want to estimate the probability of having fixed points for ϕ_1 (or ϕ_2). Such points satisfy the equation $\phi_1(x) = x$, which is equivalent of XORing $\omega + 1$ unknown vectors having length ℓ bits, whose sum equals 0. If x is randomly chosen from $\mathbb{F}_2^\ell$, then the probability of occurring $\phi_1(x) = x$ is equal to $\frac{1}{2}$. Actually, the line entries of the underlying matrix of ϕ_1 and x can be associated to independent random variables $(Z_i^{(j)})$ defined over $\{0, 1\}$, respectively, where $i \in \{1, \cdots, \omega + 1\}$ and $j \in \{1, \cdots, \ell\}$ are the column and line positions. With this setting, we have $\Pr\left[Z_i^{(j)} = 1\right] = \theta = \frac{1}{2}$. Using lemma 4 we obtain

$$\Pr\left[\sum_{i=1}^{\omega+1} Z_i^{(j)} \equiv 0 \mod 2\right] = \frac{1}{2}, \ \forall j \in \{1, \cdots, \ell\}. \tag{11}$$

and hence

$$\Pr\left[\phi_1(x) = x\right] = \left(\frac{1}{2}\right)^\ell = \frac{1}{2^\ell} \tag{12}$$

That means that the probability of occurring fixed points during the key stream generation is negligible when ℓ is chosen large enough. In this work, the values of ℓ is at least 128.

7 Experimental Results

The SBS stream cipher described above has been implemented using C/C++ programming language running on an AMD Phenom(tm) 9950 Quad-Core Processor, running at a clock rate of 1300 MHz and having 4 GB RAM. The implementation is based on random binary codes without any particular structure and makes use of C/C++-Intrinsics. Taking into account all previously discussed attacks, we have selected a large set of secure parameters providing better performance measured in cycles per byte (cpb). Table 1. illustrates the simulation results of different parameters sets (η, ℓ, ω) in which the provided security levels (in $\log_2$ binary operations), the sizes of the secret key K and the initial vector IV, and the speed are listed. In order to increase the performance and decrease the storage capacity required by our proposal, one can introduce quasi-cyclic codes due to the randomness property obtained in [20].

security	η	ℓ	ω	K/IV size	performance (cpb)
80	8192	256	32	128	7.85
100	8192	384	48	192	12.63
100	8192	512	64	256	21.13
100	8192	640	80	320	26.90
100	8192	1024	128	512	29.56
120	12288	384	48	192	12.29
160	16384	512	64	256	35.40
200	20480	640	80	320	26.819
240	24576	768	96	384	32.413
280	28672	896	112	448	39.59
260	32768	1024	128	512	29.867

Table 1. Parameters and performance of the SBS stream cipher.

In addition, our software results reported in Table 1. clearly shows that our proposal runs as fast as the AES encryption scheme in counter mode. Indeed, the assembly implementation of AES in CTR mode due to Käsper et al. [24] provides a speed of 7.59 cycles per byte on a Intel Core 2 Q9550 and 6.92 cycles per byte on Core i7 920, while our software implementation runs at 7.85 cycles per byte. Furthermore, our proposal is only about two times slower than the eSTREAM finalists [5] (HC-128, Rabbit, Salsa20/12, SOSEMANUK, Grain v1, MICKEY v2, and Trivium).

Compared to the performance of others code-based proposals, namely the SYND [19] and the 2SC [26] stream ciphers, our implementation confirms that for comparable security levels the SBS runs faster, even for the improved versions in [15].

The reported speeds of SYND [19] and the 2SC [26] are displayed in Table 2 and Table 3, respectively.

8 Conclusion

In this paper, we proposed a new code-based stream cipher, called the SBS cipher. By using parallelization, our scheme is very fast compared to all previous code-based proposals. Its security is based on the regular

[5] http://www.ecrypt.eu.org/stream/phase3perf/2007a/amd64/

security	η	ℓ	ω	key/IV size	claimed performance (cpb)
80	8192	256	32	128	27
128	8192	384	48	192	47
180	8192	512	64	256	41.50
400	8192	1024	128	512	83

Table 2. Claimed performance of the SYND stream cipher [19, 15].

security	n	r	w	key/IV size	performance (cpb)
100	1572864	384	24	144	25.18
160	2228224	544	34	208	33.22
250	3801088	928	58	352	72

Table 3. Parameters and performance of 2SC cipher given in [26, 15].

syndrome decoding problem and its performance is comparable to the AES-CTR, it runs at 7.8 cycles per byte, while the performance of the AES-CTR is about 7.59 cycles per byte. We have performed detailed security analysis, in particular, we showed that the SBS is secure against the best known attacks such as ISD attacks and GBA attacks. Moreover, we proved that distinguishing the keystream generated by SBS is as hard as solving an instance of the regular syndrome decoding problem. We encourage the readers to analyze the security of SBS.

References

1. W. Alexi, B. Chor, O. Goldreich, and C. P. Schnorr. RSA and Rabin functions: certain parts are as hard as the whole. *SIAM J. Comput.*, 17(2):194–209, 1988.
2. D. Augot, M. Finiasz, P. Gaborit, S. Manuel, and N. Sendrier. SHA-3 proposal: FSB. Submission to the SHA-3 NIST competition, 2008.
3. D. Augot, M. Finiasz, and N. Sendrier. A Family of Fast Syndrome Based Cryptographic Hash Functions. In E. Dawson and S. Vaudenay, editors, *Mycrypt 2005*, volume 3715, pages 64–83. Springer, 2005.
4. M. Bellare and D. Micciancio. A new paradigm for collision-free hashing: incrementality at reduced cost. In *Proceedings of the 16th annual international conference on Theory and application of cryptographic techniques*, EUROCRYPT'97, pages 163–192. Springer, 1997.
5. C. Berbain, H. Gilbert, and J. Patarin. QUAD: A multivariate stream cipher with provable security. *J. Symb. Comput.*, 44(12):1703–1723, 2009.
6. T. Berger, P.-L. Cayrel, P. Gaborit, and A. Otmani. Reducing key length of the mceliece cryptosystem. In *Proc. of the 2nd International Conference on Cryptology in Africa: Progress in Cryptology*, AFRICACRYPT '09, pages 77–97. Springer, 2009.
7. E. Berlekamp, R. McEliece, and H. van Tilborg. On the Inherent Intractability of Certain Coding Problems. *IEEE Trans. Inform. Theory*, 24(3):384–386, 1978.
8. D. J. Bernstein. Better price-performance ratios for generalized birthday attacks. In *Workshop Record of SHARCS07: Special-purpose Hardware for Attacking Cryptographic Systems (2007)*, 2007.
9. D. J. Bernstein. Grover vs. McEliece. In *PQCrypto*, volume 6061 of *LNCS*, pages 73–80. Springer, 2010.
10. D. J. Bernstein, J. Buchmann, and E. Dahmen. *Post Quantum Cryptography.* Springer, 1st edition, 2008.
11. D. J. Bernstein, T. Lange, C. Peters, and P. Schwabe. Really fast syndrome-based hashing. In A. Nitaj and D. Pointcheval, editors, *Progress in Cryptology–AFRICACRYPT 2011*, volume 6737 of *LNCS*, pages 134–152. Springer, 2011. `http://cryptojedi.org/papers/\#rfsb`.
12. L. Blum, M. Blum, and M. Shub. A simple unpredictable pseudo random number generator. *SIAM J. Comput.*, 15(2):364–383, 1986.
13. M. Blum and S. Micali. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM J. Comput.*, 13(4):850–864, 1984.

14. P.-L. Cayrel and M. Meziani. Post-quantum cryptography: code-based signatures. In *Proceedings of the 2010 international conference on Advances in computer science and information technology*, pages 82–99. Springer-Verlag, 2010.
15. P.-L. Cayrel, M. Meziani, O. Ndiaye, and Q. Santos. Efficient software implementations of code-based hash functions and stream-ciphers. In Çetin Kaya Koç, Sihem Mesnager, and Erkay Savas, editors, *Arithmetic of Finite Fields*, volume 9061 of *LNCS*, pages 187–203. Springer International Publishing, 2015.
16. H. Dinh, C. Moore, and A. Russell. McEliece and Niederreiter cryptosystems that resist quantum Fourier sampling attacks. In *Proceedings of the 31st annual conference on Advances in cryptology*, CRYPTO'11. Springer-Verlag, 2011.
17. M. Finiasz and N. Sendrier. Security Bounds for the Design of Code-based Cryptosystems. In Mitsuru Matsui, editor, *Advances in Cryptology - ASIACRYPT 2009*, number 5912 in LNCS, pages 88–105. Springer, 2009.
18. J.-B. Fischer and J. Stern. An efficient pseudo-random generator provably as secure as syndrome decoding. In *EUROCRYPT'96: Proc. of the 15th annual international conference on Theory and application of cryptographic techniques*, pages 245–255. Springer, 1996.
19. P. Gaborit, C. Laudaroux, and N. Sendrier. SYND: a Very Fast Code-Based Cipher Stream with a Security Reduction. In *IEEE Conference, ISIT'07*, pages 186–190, Nice, France, July 2007.
20. P. Gaborit and G. Zémor. Asymptotic improvement of the gilbert-varshamov bound for linear codes. volume abs/0708.4164, 2007.
21. O. Goldreich, R. Impagliazzo, L. Levin, R. Venkatesan, and D. Zuckerman. Security preserving amplification of hardness. In *Proceedings of the 31st Annual Symposium on Foundations of Computer Science*, SFCS '90, pages 318–326 vol.1. IEEE Computer Society, 1990.
22. O. Goldreich and L. A. Levin. A hard-core predicate for all one-way functions. In *STOC '89: Proc. of the twenty-first annual ACM symposium on Theory of computing*, pages 25–32. ACM, 1989.
23. B. S. Kaliski. *Elliptic Curves and Cryptography: A Pseudorandom Bit Generator and Other Tools.* Phd thesis, MIT, Cambridge, MA, USA, 1988.
24. E. Käsper and P. Schwabe. Faster and timing-attack resistant AES-GCM. In Christophe Clavier and Kris Gaj, editors, *Cryptographic Hardware and Embedded Systems – CHES 2009*, volume 5747 of *LNCS*, pages 1–17. Springer, 2009.
25. A. May, A. Meurer, and E. Thomae. Decoding random linear codes in $O(2^{0.054n})$. In *Proceedings of the 17th international conference on The Theory and Application of Cryptology and Information Security*, ASIACRYPT'11, pages 107–124. Springer-Verlag, 2011.
26. M. Meziani, P.-L. Cayrel, and S. M. Alaoui El Yousfi. 2SC: An Efficient Code-Based Stream Cipher. In *ISA*, volume 200 of *Communications in Computer and Information Science*, pages 111–122. Springer, 2011.
27. M. Meziani, G. Hoffmann, and P.-L. Cayrel. Improving the performance of the SYND stream cipher. In Aikaterini Mitrokotsa and Serge Vaudenay, editors, *AFRICACRYPT*, volume 7374 of *LNCS*, pages 99–116. Springer, 2012.
28. L. Minder and A. Sinclair. The extended k-tree algorithm. In *Proc. of the twentieth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA'09, pages 586–595, 2009.
29. R. Niebuhr, P.-L. Cayrel, and J. Buchmann. Improving the efficiency of Generalized Birthday Attacks against certain structured cryptosystems. In *WCC 2011*, LNCS, pages 163–172. Springer, Apr 2011.
30. E. Prange. The use of information sets in decoding cyclic codes. In *Information Theory, IRE Trans.*, volume 8, pages 5–9, 1962.
31. M.-J. O. Saarinen. Linearization attacks against syndrome based hashes. In K. Srinathan, C. Pandu Rangan, and Moti Yung, editors, *INDOCRYPT*, volume 4859 of *LNCS*, pages 1–9. Springer, 2007.
32. N. Sendrier. Code-based cryptography. In *Encyclopedia of Cryptography and Security (2nd Ed.)*, pages 215–216. Springer, 2011.
33. P. W. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In *SFCS '94: Proc. of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE Computer Society, 1994.
34. D. Wagner. A generalized birthday problem. In Moti Yung, editor, *CRYPTO*, volume 2442 of *LNCS*. Springer, 2002.
35. A. C. Yao. Theory and applications of trapdoor functions (extended abstract). In *FOCS*, pages 80–91. IEEE Computer Society, 1982.

PAC: Polytopes Algebra Computation

Session Organizers

Zafeirakis Zafeirakopoulos
University of Athens
zafeirakopoulos@gmail.com

Felix Breuer
Research Institute for Symbolic Computation in Linz
felix@felixbreuer.net

Overview

The special session on Polytopes-Algebra-Computation will focus on the interaction of polyhedral geometry with algebra and algebraic geometry from a computational viewpoint.

A geometric approach for the upper bound theorem for Minkowski sums of convex polytopes

Eleni Tzanaki

We derive tight expressions for the maximum number of k-faces, $0 \leq k \leq d-1$, of the Minkowski sum, $P_1 + \cdots + P_r$, of r convex d-polytopes $P_1, \ldots, P_r$ in R^d, where $d \geq 2$ and $r < d$, as a (recursively defined) function on the number of vertices of the polytopes. To prove our results, we use basic notions such as f - and h-vector calculus, stellar-subdivisions and shellings, and generalize the steps used by McMullen to prove the Upper Bound Theorem for polytopes. The key idea behind our approach is to express the Minkowski sum $P_1 + \cdots + P_r$ as a section of the Cayley polytope C of the summands; bounding the k-faces of $P_1 + \cdots + P_r$ reduces to bounding the subset of the $(k+r-1)$-faces of C that contain vertices from each of the r polytopes. In the case where $r < d$, we provide an explicit construction which attains the upper bound.

A sparse implicitisation framework

Christos Konaxis

Based on the computation of the so called predicted polytope Q, containing the Newton polytope P of the implicit equation, implicitization of a parametric hypersurface is reduced to computing the nullspace of a numeric interpolation matrix. Our approach predicts Q by exploiting the sparseness of the given parametric equations and of the implicit polynomial, without being affected by the presence of any base points.

We describe two approaches in constructing the interpolation matrix. The main method, given a superset of the monomials in the implicit polynomial, constructs the matrix by evaluating these monomials at points on the object. The second method uses the linear relations between the implicit and the parametric expressions of the normal to the curve or surface at any given point and works either with parameterized objects or with objects given by a point cloud along with normals at the points. The matrix dimension is not smaller than the main method, but the number of sample points required to construct it can be reduced up to one third.

When the predicted polytope Q contains P as a Minkowski summand, we improve the efficiency of the method by employing Minkowski decomposition to detect the Minkowski summand of Q relevant to implicitization. We design and implement in Sage a new, public domain, practical, potentially generalizable and worst-case optimal algorithm for Minkowski decomposition in 3D based on integer linear programming.

Finally, we study how the interpolation matrix expresses the implicit equation as a matrix determinant, which is useful for certain operations such as ray shooting, and how it can be used to reduce some key geometric predicates on the hypersurface, namely membership and sidedness for given query points, to simple numerical operations on the matrix, without need to develop the implicit equation.

This is joint work with I. Emiris, T. Kalinka, and Z. Zafeirakopoulos

Normal lattice polytopes

Winfried Bruns

Normal lattice polytopes can be considered as the discrete analogue of compact convex sets. In algebraic geometry they represent projectively normal toric varieties, and in commutative algebra they correspond to standard graded normal monoid algebras. They provide an ideal testing ground for these areas, both theoretically and experimentally.

We give a survey of challenging solved and open problems on lattice polytopes and report on recent work with Joseph Gubeladze and Mateusz Michalek. The challening problems include unimodular covering and triangulation, the integral Caratheodory property and the normality of smooth polytopes. The recent work deals with the extendability of normal polytopes by elementary "jumps" and the existence of maximal normal polytopes.

Enumeration of 2-level polytopes

Vissarion Fisikopoulos

We propose the first algorithm for enumerating all combinatorial types of 2-level (a.k.a. compressed) polytopes of a given dimension d, and provide complete experimental results for $d \leq 6$. Our approach is based on new findings on 2-level polytopes, also presented here. In particular, we introduce the notion of a simplicial core, which allows us to reduce the problem to the enumeration of the closed sets of a discrete closure operator, along with some convex hull computations and isomorphism tests.

Joint work with: Adam Bohn, Yuri Faenza, Samuel Fiorini, Marco Macchia, Kanstantsin Pashkovich

Recent developments in Normaliz

Christof Söger

Normaliz is a well-established computer program for rational cones and polytopes. Its main computation goals are Hilbert bases and Ehrhart series. It has interfaces to computer algebra systems (CoCoA, GAP, Macauly 2, Singular) and to polymake. We give an overview of the program and discuss recent extensions, in particular the new features of Normaliz 3.0.

Starting cones for tropical traversals

Anders Jensen

The tropical variety of a prime polynomial ideal is a pure, connected polyhedral fan, that may be computed by traversal. To start this traversal a single cone is required. So far no good method for finding a starting cone was known. In this talk we propose to find one by stably intersecting with coordinate hyperplanes until a tropical curve is obtained. The key idea is that doing stable intersections translates into doing Groebner basis computations over a field of rational functions. Using a recursive reformulation of Chan's tropical curve algorithm, finding a single ray in a curve is often easy. The tropical cone is then obtained by repeatedly finding such rays according to an already known heuristic strategy for tropical cone construction.

Computing the Chern-Scwrartz-MacPherson Class and Euler Characteristic of Complete Simplical Toric Varieties

Martin Helmer[1]

[1] *University of Western Ontario, Canada,* mhelmer2@uwo.ca.
Webpage: http://publish.uwo.ca/~mhelmer2/

In this note we present Algorithm 2.1, a combinatorial algorithm which computes the Chern-Schwartz-MacPherson (c_{SM}) class and/or the Euler characteristic of a complete simplicial toric variety X_Σ defined by a fan Σ (that is we allow X_Σ to have finite quotient singularities). The algorithm is based on a result of Barthel, Brasselet and Fieseler [1] which gives an expression for the c_{SM} class of a toric variety in terms of torus orbit closures. Note that we will only consider toric varieties X_Σ over the complex numbers $\mathbf{C}$.

We also note that the restriction to complete simplicial toric varieties is not required in the statement of the result of Barthel, Brasselet and Fieseler [1] on which our algorithm is based, indeed these restrictions are present on the algorithm only for the purpose of simplifying the construction of the Chow ring of the toric variety. If one was able to construct the Chow ring in a simple manner with the restrictions removed the algorithm could be applied unchanged in this more general setting.

The Macaulay2 [3] implementation of our algorithm for computing the c_{SM} class and Euler characteristic of a complete simplicial toric variety presented in this note can be found at `https://github.com/Martin-Helmer/char-class-calc`. This implementation is accessed via the “CharToric" package.

1 Setting and Notation

Let X_Σ be a n-dimensional complete and simplicial toric variety; then the intersection product can be defined on rational cycles (see §12.5 of [2]) so that, if we let $\mathbf{Q}$ denote the rational numbers and $\mathbf{Z}$ the integers, we have that the rational Chow ring of X_Σ is given by the graded ring

$$A^*(X_\Sigma)_{\mathbf{Q}} = A^*(X_\Sigma) \otimes_{\mathbf{Z}} \mathbf{Q} = \bigoplus_{j=0}^{n} A^j(X_\Sigma) \otimes_{\mathbf{Z}} \mathbf{Q}. \tag{1}$$

For each cone σ in the fan Σ the orbit closure $V(\sigma)$ is a subvariety of codimension dim(σ). We will write $[V(\sigma)]$ for the rational equivalence class of $V(\sigma)$ in $A^{\dim(\sigma)}(X_\Sigma)$.

Proposition 1.1 (Lemma 12.5.1 of [2]) *The collections $[V(\sigma)] \in A_j(X_\Sigma)$ for $\sigma \in \Sigma$ having dimension $n-j$ generate $A_j(X_\Sigma)$, the Chow group of dimension j. Further the collection $[V(\sigma)]$ for all $\sigma \in \Sigma$ generates $A^*(X_\Sigma)$ as an abelian group.*

The following proposition gives us a simple method to compute the rational Chow ring of a complete, simplicial toric variety X_Σ.

Proposition 1.2 (Theorem 12.5.3 of Cox, Little, Schenck [2]) *Let N be an integer lattice with dual M. Let X_Σ be a complete and simplicial toric variety with generating rays $\Sigma(1) = \rho_1, \dots, \rho_r$ where $\rho_j = \langle v_j \rangle$ for $v_j \in N$. Then we have that*

$$\mathbf{Q}[x_1, \dots, x_r]/(\mathscr{I} + \mathscr{J}) \cong A^*(X_\Sigma)_{\mathbf{Q}}, \tag{2}$$

with the isomorphism map specified by $[x_i] \mapsto [V(\rho_i)]$. Here $\mathscr{I}$ denotes the Stanley-Reisner ideal of the fan Σ, that is the ideal in $\mathbf{Q}[x_1, \dots, x_r]$ specified by

$$\mathscr{I} = (x_{i_1} \cdots x_{i_s} \mid i_{i_j} \text{ distinct and } \rho_{i_1} + \cdots + \rho_{i_s} \text{ is not a cone of } \Sigma) \tag{3}$$

and J denotes the ideal of $\mathbf{Q}[x_1, \dots, x_r]$ generated by linear relations of the rays, that is $\mathscr{J}$ is generated by linear forms

$$\sum_{j=1}^{r} m(v_j) x_j \tag{4}$$

for m ranging over some basis of M.

2 Algorithm

In this section we present Algorithm 2.1 which computes the c_{SM} class and/or Euler characteristic of a complete simplicial toric variety defined by a fan Σ.

Proposition 2.1 (Main Theorem of Barthel, Brasselet and Fieseler [1]) *Let X_Σ be an n-dimensional complex toric variety specified by a fan Σ. We have that the Chern-Schwartz-MacPherson class of X_Σ can be written in terms of orbit closures as*

$$c_{SM}(X_\Sigma) = \sum_{\sigma \in \Sigma} [V(\sigma)] \quad \in A^*(X_\Sigma)_{\mathbf{Q}} \tag{5}$$

where $V(\sigma)$ is the closure of the torus orbit corresponding to σ.

Lemma 2.2 is a modified version of Proposition 11.1.8. of Cox, Little, Schenck [2], it will allow us to compute the multiplicity of a simplicial cone. We have slightly altered the statement of the result to explicitly show how we will compute these multiplicities in practice.

Lemma 2.2 (Modified version of Proposition 11.1.8. of Cox, Little, Schenck [2]) *Let $N = \mathbf{Z}^n$ be an integer lattice. For a simplicial cone $\sigma = \rho_1 + \cdots + \rho_d \subset N$ let M_σ be the matrix with columns specified by the generating vectors of the rays $\rho_1, \ldots, \rho_d$ which define the cone σ; we have*

$$\mathrm{mult}(\sigma) = |\det(\mathrm{Herm}(M_\sigma))| \tag{6}$$

where $\mathrm{Herm}(M_\sigma)$ *denotes the Hermite normal form of matrix M_σ with all zero rows and/or zero columns removed. Further* $\mathrm{mult}(\sigma) = 1$ *if and only if U_σ is smooth.*

To compute the classes $[V(\sigma)]$ appearing in (5) we will employ the following proposition combined with Proposition 1.2.

Proposition 2.3 (Theorem 12.5.2. of Cox, Little, Schenck [2]) *Assume that X_Σ is complete and simplicial. If $\rho_1, \ldots, \rho_d \in \Sigma(1)$ are distinct and if $\sigma = \rho_1 + \cdots + \rho_d \in \Sigma$ then in $A^*(X_\Sigma)$ we have the following:*

$$[V(\sigma)] = \mathrm{mult}(\sigma)[V(\rho_1)] \cdot [V(\rho_2)] \cdots [V(\rho_d)]. \tag{7}$$

Here $\mathrm{mult}(\sigma)$ *will be calculated using Lemma 2.2.*

In Algorithm 2.1 we present an algorithm to compute $c_{SM}(X_\Sigma)$ for a complete, simplicial toric variety X_Σ defined by a fan Σ. Note that we represent $[V(\rho_j)]$ as x_j using the isomorphism in Proposition 1.2.

Algorithm 2.1 ***Input:*** *A complete, simplicial toric variety X_Σ defined by a fan Σ with $\Sigma(1) = \{\rho_1, \ldots, \rho_r\}$ and a boolean, Euler_only, indicating if only the Euler characteristic is desired. We assume* $\dim(X_\Sigma) \geq 1$.
Output: *$c_{SM}(X_\Sigma)$ in $A^*(X_\Sigma)_{\mathbf{Q}} \cong \mathbf{Q}[x_1, \ldots, x_r]/(\mathscr{I} + \mathscr{J})$ and/or the Euler characteristic $\chi(X_\Sigma)$, if Euler_only=true then only $\chi(X_\Sigma)$ will be computed.*

```
• Compute the rational Chow ring $A^*(X_\Sigma)_{\mathbf{Q}} \cong \mathbf{Q}[x_1, \ldots, x_r]/(\mathscr{I} + \mathscr{J})$ using
  Proposition 1.2.
• csm = 0.
• For i from $\dim(X_\Sigma)$ to 1:
    ◦ orbits = all subsets of $\Sigma(1) = \{\rho_1, \ldots, \rho_r\}$ containing i elements.
    ◦ total = 0.
    ◦ For $\rho_{j_1}, \ldots, \rho_{j_s}$ in orbits:
        ◇ $\sigma = \rho_{j_1} + \cdots + \rho_{j_s}$.
        ◇ Find $w = \mathrm{mult}(\sigma)$ using Lemma 2.2.
        ◇ $[V(\sigma)] = \mathrm{mult}(\sigma)[V(\rho_{i_1})]\cdots[V(\rho_{i_s})] = w\cdot x_{i_1}\cdots x_{i_s}$.
        ◇ $\mathrm{total} = \mathrm{total} + [V(\sigma)]$.
    ○ $\mathrm{csm} = \mathrm{csm} + \mathrm{total}$.
    ○ If $i == \dim(X_\Sigma)$:
        ◇ Set $(c_{SM}(X_\Sigma))_0 = \mathrm{csm}$.
        ◇ Set $\chi(X_\Sigma)$ = sum of the coefficients of the monomials in $(c_{SM}(X_\Sigma))_0$.
        ◇ If Euler_only==true:
            ▷ Return $\chi(X_\Sigma)$.
• Set $c_{SM}(X_\Sigma) = \mathrm{csm}$.
• Return $c_{SM}(X_\Sigma)$ and/or $\chi(X_\Sigma)$ .
```

We note that Algorithm 2.1 is strictly combinatorial; hence the runtime depends only on the combinatorics of the fan Σ defining the toric variety.

3 Performance

In this section we give the run times for Algorithm 2.1 applied to a variety of examples. Consider a complete simplicial toric variety X_Σ. We give two alternate implementations of Algorithm 2.1 to reflect what we can expect the timings to be in both the smooth cases and singular cases.

Specifically the running times in Table 1 for Algorithm 2.1 marked with a † check the input to see if the given fan Σ defines a smooth toric variety, if it does these implementations use the fact that $\mathrm{mult}(\sigma) = 1$ for all $\sigma \in \Sigma$ and hence do not compute the Hermite normal forms and their determinates in Lemma 2.2. However to show how the algorithm would perform on a singular input of a similar size and complexity we also give running times for an implementation which always computes the Hermite forms and their determinates in Lemma 2.2. In this way we see in a precise manner what the extra cost associated to computing the c_{SM} class and Euler characteristic of a singular toric variety would be in comparison to the cost of computing a smooth toric variety defined by a fan having similar combinatorial structure.

By default the implementation of Algorithm 2.1 in our "CharToric" package checks if the input defines a smooth toric variety, i.e. performs the procedure of the implementations marked with †.

We also remark that the extra cost in the singular case (or in the case where we don't check the input) comes entirely from performing linear algebra with integer matrices. As such the running times in these cases could perhaps be somewhat reduced by using a specialized integer linear algebra package. To give a rough quantification of what performance improvement one might expect from this we performed some testing using LinBox [4] and PARI [6] via Sage [5] on linear systems of similar size and structure to those arising in the examples in Table 1. In this testing we found that the specialized algorithms seemed to be around two to three times faster than the linear algebra methods used by our implementation in the “CharToric" package, however this testing is by no means conclusive.

Input	Alg. 2.1 †	Alg. 2.1 (Euler only) †	Alg. 2.1	Alg. 2.1 (Euler only)	Chow Ring (Prop. 1.2)
$\mathbf{P}^6$	0.0s	0.0s	0.0s	0.0s	0.1 s
$\mathbf{P}^{16}$	5.3s	0.0s	85.4s	0.0s	0.7 s
$\mathbf{P}^5 \times \mathbf{P}^6$	0.3s	0.0s	3.7s	0.0s	1.2 s
$\mathbf{P}^5 \times \mathbf{P}^8$	1.1s	0.0s	16.8s	0.1s	2.1 s
$\mathbf{P}^8 \times \mathbf{P}^8$	12.0s	0.1s	168.5s	0.1s	4.5 s
$\mathbf{P}^5 \times \mathbf{P}^5 \times \mathbf{P}^5$	12.8s	0.2s	156.7s	0.6s	11.8 s
$\mathbf{P}^5 \times \mathbf{P}^5 \times \mathbf{P}^6$	28.4s	0.3s	387.1s	0.8s	17.0 s
Fano sixfold 123	0.3s	0.0s	1.0s	0.4s	1.1 s
Fano sixfold 1007	0.4s	0.1s	1.0s	0.1s	1.8 s

Table 1: Note that the table we present the time to compute the Chow ring seperately from the time reqired for the other computations, as such the total run time for each algorithm will be the time listed in its column plus the time to compute the Chow ring if the Chow ring is not already known. Computations were performed using Macaulay2 [3] on a computer with a 2.9GHz Intel Core i7-3520M CPU and 8 GB of RAM. The Fano sixfolds are those built by the smoothFanoToricVariety method in the “NormalToricVarieties" Macaulay2 [3] package. $\mathbf{P}^n$ denotes a projective space of dimension n

References

[1] Gottfried Barthel, J-P Brasselet, and K-H Fieseler. Classes de Chern de variétés toriques singulières. *Comptes rendus de l'Académie des sciences. Série 1, Mathématique*, 315(2):187–192, 1992.

[2] David A. Cox, John B. Little, and Henry K. Schenck. *Toric varieties*, volume 124. American Mathematical Soc., 2011.

[3] Daniel R. Grayson and Michael E. Stillman. *Macaulay2, a software system for research in algebraic geometry*, 2013.

[4] The LinBox Group. *LinBox – Exact Linear Algebra over the Integers and Finite Rings, Version 1.1.6*, 2008.

[5] W. A. Stein et al. *Sage Mathematics Software (Version 5.11).* The Sage Development Team, 2013. `http://www.sagemath.org`.

[6] The PARI Group, Bordeaux. *PARI/GP version* `2.7.0`, 2014. available from `http://pari.math.u-bordeaux.fr/`.

Gröbner Bases, Resultants and Linear Algebra

Session Organizers

Maximilian Jaroschek
Max-Planck-Institut fr Informatik
mjarosch@mpi-inf.mpg.de

Zafeirakis Zafeirakopoulos
University of Athens
zafeirakopoulos@gmail.com

Overview

GBReLA 2 is a special session at the conference for Applications of Computer Algebra (ACA) 2015. Its theme lies in the intersection of Gröbner bases, resultants and linear algebra. The talks will range from comprehensible introductions to recent research results and ideas. Beginners in this area will have the chance to dive into the linear algebra approach to Gröbner bases and resultants, while advanced students and researchers will have the chance to learn about new insights into the connections of Gröbner bases, resultants and related matrix methods.

A Brief Introduction to the Extended Linearization Method (or XL Algorithm) for Solving Polynomial Systems of Equations

Gregory V. Bard[1]

[1] *University of Wisconsin—Stout, Wisconsin, USA, bardg@uwstout.edu*

While it works over any coefficient field, the XL Algorithm was developed to solve polynomial systems of equations mod 2. Such polynomial systems arise during the cryptanalysis of many ciphers [10]. The XL algorithm has been the subject of numerous papers since its original appearance [4] [5] [6] [7] [8] [9], and the algorithm featured in the Ph.D. dissertation of Nicolas Courtois [3].

The algorithm can be thought of as converting the original polynomial system of equations into an enormous linear algebra problem. Each monomial of the polynomial system becomes a variable in the linear system, and thus a column in the XL matrix [10]. The equations are each multiplied by all possible monomials of degree up to some fixed degree, generating a very large number of rows. One then computes the RREF of the resulting matrix. If certain parameters are carefully chosen at the start, then the solution to the polynomial system will be obtained.

This also leads to an interesting paradox, an exciting connection to the theory of NP-Completeness. Computing the RREF of a matrix is a cubic-time (or faster) problem, but solving a polynomial system of equations is an NP-Complete problem. How then, can the act of solving a polynomial system, which is believed to be very hard, be reduced to the act of solving a linear system, which is believed to be very easy? This seems to imply $P = NP$, which would be a surprise. The resolution of this paradox is that the matrix is so large, that its size is exponentially large in comparison to the original polynomial system of equations. This is the origin of the name, “XL,” as it stands for eXtended Linearization, but is also the designation that means “extra large” for items of clothing.

There are several successor algorithms that are enhancements of the XL algorithm, including MutantXL [13] [2] [11]. The F4 family of algorithms, discovered independently by Jean-Charles Faugere [12], and his coauthors, can also be shown to be equivalent (or very similar) to the XL algorithm in many cases, and has many follow-on papers as well.

To be concise, this talk will focus only on the original XL paper (making the talk extremely well-suited to beginners), and if time permits, the connections to NP-Completeness will be sketched, but there will not be time for proofs. Further information on the XL family of algorithms can be found in Chapter 12.4, “The XL

Algorithm," of *Algebraic Cryptanalysis* [1], a monograph written by the speaker, and published by Springer in 2009.

References

[1] G. Bard, *Algebraic Cryptanalysis*, Springer, 2009.

[2] J. Buchmann, J. Ding, M. S. E. Mohamed, and W. S. A. E. Mohamed. "MutantXL: Solving Multivariate Polynomial Equations for Cryptanalysis." Dagstuhl seminar proceedings Report No. 09031. 2009.

[3] N. Courtois. *The security of cryptographic primitives based on multivariate algebraic problems: MQ, MinRank, IP, HFE*. Ph.D. Thesis, University of Paris VI (2001).
Available at `http://www.nicolascourtois.net/phd.pdf`

[4] N. Courtois. "The security of Hidden Field Equations (HFE)." Proceedings of the CryptographersÕ Track, RSA Conference, (RSA'01). *Lecture Notes in Computer Science*, **Vol. 2020**. Springer, 2001. Pp. 266–281.

[5] N. Courtois. "Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt." Proceedings of International Conference on Information Security and Cryptology (ICSC'02), *Lecture Notes in Computer Science*, **Vol. 2587**. Springer, 2002. Pp. 182–199.

[6] N. Courtois. "Fast algebraic attacks on stream ciphers with linear feedback." Advances in Cryptology—Proceedings of (CRYPTO'03), *Lecture Notes in Computer Science*, **Vol. 2729**. Springer, 2003. Pp. 176–194.

[7] N. Courtois. "Generic attacks and the security of Quartz." Public Key Cryptography (PKCÕ03). *Lecture Notes in Computer Science*, **Vol. 2567**. Springer, 2003. Pp. 351–364.

[8] N. Courtois. "Algebraic attacks on combiners with memory and several outputs." Proceedings of International Conference on Information Security and Cryptology (ICISC'04). *Lecture Notes in Computer Science*, **Vol. 3506**. Springer, 2004. Pp. 3–20.

[9] . N. Courtois and G. Bard. "Algebraic cryptanalysis of the data encryption standard." Proceedings of the 11th IMA international conference on Cryptography and Coding (IMACC'07). *Lecture Notes in Computer Science*, **Vol. 4887**. Springer, 2008. Pp 152–169.

[10] N. Courtois, A. Klimov, J. Patarin, A. Shamir. "Efficient Algorithms for Solving Over-defined Systems of Multivariate Polynomial Equations." Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'00). *Lecture Notes in Computer Science*, **Vol. 1807**. Springer, 2000. Pp. 392–407.

[11] J. Ding, J. Buchmann, M.S.E. Mohamed, W.S.A. Mohamed, R. P. Weinmann. "MutantXL." Proceedings of the 1st international conference on Symbolic Computation and Cryptography (SCC'08). LMIB. 2008. Pp. 16–22.

[12] J. C. Faugere. "A new efficient algorithm for computing Groebner bases (F4)." *Pure and Applied Algebra*. **Vol. 139**. 1999. Pp. 61–88.

[13] M. S. E. Mohamed, W. S. A. E. Mohamed, J. Ding, J. Buchmann. "MXL2: Solving Polynomial Equations over GF(2) using an Improved Mutant Strategy." Proceedings of The Second international Workshop on Post-Quantum Cryptography (PQCrypto'08). *Lecture Notes in Computer Science*, **Vol. 5299**. Springer, 2008. Pp. 203–215.

Gröbner Bases and Structured Systems: an overview

Jean-Charles Faugère

INRIA, Équipe POLSYS, Centre Paris – Rocquencourt,
F-75005, Paris, France.
Sorbonne Universités, UPMC Univ Paris 06, Équipe POLSYS,
LIP6, F-75005, Paris, France.
CNRS, UMR 7606, LIP6, F-75005, Paris, France.

Joint work with Jules Svartz and Pierre-Jean Spaenlehauer.

June 12, 2015

Structured systems.

A major challenge in polynomial system solving is that, in most cases, the number of solutions of a polynomial system is *exponential*. Moreover, in finite fields, solving polynomial systems is a NP-hard problem. However problems coming from applications usually have additional structures. Consequently, a fundamental issue is to design a new generation of algorithms exploiting the special structures that appear ubiquitously in the applications.

At first glance, multi-homogeneity, weighted homogeneity (quasi-homogeneity), overdeterminedness, sparseness and symmetries seem to be unrelated structures. Indeed, until recently we have obtained specific results for one type of structure: we obtain dedicated algorithm and sharp complexity results too handle a particular structure. For instance, we handle bilinear systems by reducing the problem to determinantal ideals; we also propose ad-hoc techniques to handle symmetries. We show that Gröbner bases for weighted homogeneous systems can be computed by adapting existing algorithms.

All these results have been obtained *separately* by studying each structure one by one. Recently we found a new unified way to analyze these problems based on monomial sparsity. To this end, we introduce a new notion of sparse Gröbner bases, an analog of classical Gröbner bases for semigroup algebras. We propose sparse variants of the F_4/F_5 and FGLM algorithms to compute them and we obtain new and sharp estimates on the complexity of solving them (for zero-dimensional systems where all polynomials share the same Newton polytope). As a by product, we can generalize to the multihomogeneous case the already useful bounds obtained in the bilinear case. We can now handle in a uniform way several type of structured systems (at least when the type of structure is the same for every polynomial). From a practical point of view, all these results lead to a striking improvement in the execution time.

More recently, we investigate the non convex case when only a small subset of monomials appear in the equations: the emphfewnomial case. We can relate the complexity of solving the corresponding algebraic system with some combinatorial property of a graph associated with the support of the polynomials. We show that, in some cases, the systems can be solved in polynomial time.

On the complexity of polynomial reduction*

Joris van der Hoeven

LIX, CNRS
École polytechnique
91128 Palaiseau Cedex
France

Email: vdhoeven@lix.polytechnique.fr
Web: http://lix.polytechnique.fr/~vdhoeven

May 30, 2015

Sparse interpolation [1, 3, 2, 10] provides an interesting paradigm for efficient computations with multivariate polynomials. In particular, under suitable hypothesis, multiplication of sparse polynomials can be carried out in quasi-linear time, in terms of the expected output size. More recently, other multiplication algorithms have also been investigated, which outperform naive and sparse interpolation under special circumstances [11, 9]. An interesting question is how to exploit such algorithms for accelerating other operations. In this paper, we will focus on the reduction of a multivariate polynomial with respect to an autoreduced set of other polynomials and show that fast multiplication algorithms can indeed be exploited in this context in an asymptotically quasi-optimal way.

Consider the polynomial ring $\mathbb{K}[x] = \mathbb{K}[x_1, \ldots, x_n]$ over an effective field $\mathbb{K}$ with an effective zero test. Given a polynomial $P = \sum_{i \in \mathbb{N}^n} P_i x^i = \sum_{i_1, \ldots, i_n \in \mathbb{N}} P_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n}$, we call $\operatorname{supp} P = \{i \in \mathbb{N}^n : P_i \neq 0\}$ the *support* of P. The naive multiplication of two sparse polynomials $P, Q \in \mathbb{K}[x]$ requires *a priori* $\mathcal{O}(|\operatorname{supp} P| \, |\operatorname{supp} Q|)$ operations in $\mathbb{K}$. This upper bound is sharp if P and Q are very sparse, but pessimistic if P and Q are dense.

Assuming that $\mathbb{K}$ has characteristic zero, a better algorithm was proposed in [2] (see also [1, 3] for some background). The complexity of this algorithm can be expressed in the expected size $s = |\operatorname{supp} P + \operatorname{supp} Q|$ of the *output* (when no cancellations occur). It is shown that P and Q can be multiplied using only $\mathcal{O}(\mathsf{M}(s) \log s)$ operations in $\mathbb{K}$, where $\mathsf{M}(s) = \mathcal{O}(s \log s \log \log s)$ stands for the complexity of multiplying two univariate polynomials in $\mathbb{K}[z]$ of degrees $<s$. Unfortunately, the algorithm in [2] has two drawbacks:

1. The algorithm leads to a big growth for the sizes of the coefficients, thereby compromising its bit complexity (which is often worse than the bit complexity of naive multiplication).
2. It requires $\operatorname{supp} P Q \subseteq \operatorname{supp} P + \operatorname{supp} Q$ to be known beforehand. More precisely, whenever a bound $\operatorname{supp} P Q \subseteq \operatorname{supp} P + \operatorname{supp} Q \subseteq \mathcal{S}$ is known, then we really obtain a multiplication algorithm of complexity $\mathcal{O}(\mathsf{M}(|\mathcal{S}|) \log |\mathcal{S}|)$.

*. This work has been supported by the ANR-09-JCJC-0098-01 MaGiX project, the Digiteo 2009-36HD grant and Région Ile-de-France.

In practice, the second drawback is of less importance. Indeed, especially when the coefficients in $\mathbb{K}$ can become large, then the computation of $\operatorname{supp} P + \operatorname{supp} Q$ is often cheap with respect to the multiplication $P\, Q$ itself, even if we compute $\operatorname{supp} P + \operatorname{supp} Q$ in a naive way.

Recently, several algorithms were proposed for removing the drawbacks of [2]. First of all, in [10] we proposed a practical algorithm with essentially the same advantages as the original algorithm from [2], but with a good bit complexity and a variant which also works in positive characterisic. However, it still requires a bound for $\operatorname{supp} P\, Q$ and it only works for special kinds of fields $\mathbb{K}$ (which nevertheless cover the most important cases such as $\mathbb{K} = \mathbb{Q}$ and finite fields). Even faster algorithms were proposed in [7, 11], but these algorithms only work for special supports. Yet another algorithm was proposed in [5, 9]. This algorithm has none of the drawbacks of [2], but its complexity is suboptimal (although better than the complexity of naive multiplication).

At any rate, these recent developments make it possible to rely on fast sparse polynomial multiplication as a building block, both in theory and in practice. This makes it natural to study other operations on multivariate polynomials with this building block at our disposal. One of the most important such operations is division.

The multivariate analogue of polynomial division is the reduction of a polynomial $A \in \mathbb{K}[x]$ with respect to an autoreduced tuple $B = (B_1, \ldots, B_b) \in \mathbb{K}[x]^b$ of other polynomials. This leads to a relation

$$A \;=\; Q_1 B_1 + \cdots + Q_b B_b + R, \tag{1}$$

such that none of the terms occurring in R can be further reduced with respect to B. In this paper, we are interested in the computation of R as well as $Q_1, \ldots, Q_b$. We will call this the problem of *extended reduction*, in analogy with the notion of an “extended g.c.d.”.

Now in the univariate context, “relaxed power series” provide a convenient technique for the resolution of implicit equations [4, 5, 6, 8]. One major advantage of this technique is that it tends to respect most sparsity patterns which are present in the input data and in the equations. The main technical tool in this paper (see section 2) is to generalize this technique to the setting of multivariate polynomials, whose terms are ordered according to a specific admissible ordering on the monomials. This will make it possible to rewrite (1) as a so called recursive equation (see section 3.2), which can be solved in a relaxed manner. Roughly speaking, the cost of the extended reduction then reduces to the cost of the relaxed multiplications $Q_1 B_1, \ldots, Q_b B_b$. Up to a logarithmic overhead, we show that this cost is the same as the cost of checking the relation (1).

References

[1] M. Ben-Or and P. Tiwari. A deterministic algorithm for sparse multivariate polynomial interpolation. In *STOC '88: Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 301–309, New York, NY, USA, 1988. ACM Press.

[2] J. Canny, E. Kaltofen, and Y. Lakshman. Solving systems of non-linear polynomial equations faster. In *Proc. ISSAC '89*, pages 121–128, Portland, Oregon, A.C.M., New York, 1989. ACM Press.

[3] D. Y. Grigoriev and M. Karpinski. The matching problem for bipartite graphs with polynomially bounded permanents is in NC. In *Proceedings of the 28th IEEE Symposium on the Foundations of Computer Science*, pages 166–172, 1987.

[4] J. van der Hoeven. Lazy multiplication of formal power series. In W. W. Küchlin, editor, *Proc. ISSAC '97*, pages 17–20, Maui, Hawaii, July 1997.

[5] J. van der Hoeven. Relax, but don't be too lazy. *JSC*, 34:479–542, 2002.

[6] J. van der Hoeven. Relaxed multiplication using the middle product. In Manuel Bronstein, editor, *Proc. ISSAC '03*, pages 143–147, Philadelphia, USA, August 2003.

[7] J. van der Hoeven. The truncated Fourier transform and applications. In J. Gutierrez, editor, *Proc. ISSAC 2004*, pages 290–296, Univ. of Cantabria, Santander, Spain, July 4–7 2004.

[8] J. van der Hoeven. New algorithms for relaxed multiplication. *JSC*, 42(8):792–802, 2007.

[9] J. van der Hoeven and G. Lecerf. On the complexity of blockwise polynomial multiplication. In *Proc. ISSAC '12*, pages 211–218, Grenoble, France, July 2012.

[10] J. van der Hoeven and G. Lecerf. On the bit-complexity of sparse polynomial multiplication. *JSC*, 50:227–254, 2013.

[11] J. van der Hoeven and É. Schost. Multi-point evaluation in higher dimensions. *AAECC*, 24(1):37–52, 2013.

The Generalized Rabinowitsch's Trick

Dingkang Wang[1], Yao Sun[2], and Jie Zhou[1]

[1] KLMM, Academy of Mathematics and Systems Science, CAS, Beijing, China
[2] SKLOIS, Institute of Information Engineering, CAS, Beijing, China

The classical Rabinowitsch trick was proposed by J.L. Rabinowitsch in his 1-page paper *Zum Hilbertschen Nullstellensatz* in 1929. This ingenious trick was used to prove the famous Hilbert's Nullstellensatz theorem. Indeed, given polynomials $f, f_1, \ldots, f_s$ in $k[x_1, \ldots, x_n]$ or $k[X]$. If f vanishes on the common zeros of $f_1, \ldots, f_s$, then there exists polynomials $a_0, a_1, \ldots, a_s$ in $k[X, y]$, such that

$$a_0(fy - 1) + a_1 f_1 + \cdots + a_s f_s = 1,$$

where y is an extra variable different from X. Substituting y by $1/f$, there exists an integer m such that f^m in the ideal which is generated by $f_1, \ldots, f_s$.

We present a generalization of Rabinoswitsch's trick, which is an integration of Rabinowitsch's trick with Bayer's idea. We consider the following polynomial ideal

$$J = I + \langle fy - z \rangle \subset k[X, y, z],$$

associated with I and f, where y and z are two new variables different from X.

We analyze the ideal J by studying its Gröbner bases using a block ordering in which $y \gg z \gg X$. Using the structure of this Gröbner bases, we give the main theoretical result as follows.

Theorem 1. *Let I be an ideal and f be a polynomial in $k[X]$. Let G be a Gröbner basis of ideal $J = I + \langle fy - z \rangle \subset k[X, y, z]$ with respect to a block ordering such that $y \gg z \gg X$.*

1. *Let $P_s = \{\mathrm{lc}_{y,z}(g) \mid g \in G \cap k[X][z], \mathrm{lpp}_{y,z}(g) = z^k \text{ and } 0 \le k \le s\} \subset k[X]$. For any integer $s \ge 0$, P_s is a Gröbner bases of $I : f^s$.*
2. *Let $Q_s = P_s \cup \{\mathrm{lc}_{y,z}(g) \mid g \in G, \mathrm{lpp}_{y,z}(g) = yz^t, \text{ and } 0 \le t \le s\} \subset k[X]$. For any integer $s \ge 0$, Q_s is a Gröbner bases of $I : f^s + \langle f \rangle$.*

The following result serves as the basis for checking if a polynomial is invertible or a zero divisor in a residue class ring as well as for checking its membership in the radical of an ideal.

Theorem 2. *Let I be an ideal and f be a polynomial in $k[X]$. Let G be a minimal Gröbner basis of ideal $J = I + \langle fy - z \rangle \subset k[X, y, z]$ with respect to a block ordering such that $y \gg z \gg X$, and P_s, Q_s are constructed from G as stated in Theorem 1. Then the following asserts hold:*

1. *f is **invertible** in $k[X]/(I : f^s)$ if and only if $1 \in Q_s$ and $1 \notin P_{s+1}$, i.e. $I : f^s + \langle f \rangle = \langle 1 \rangle$ and $f \notin I : f^s$. That is, there is a polynomial $g = yz^t + p_{t-1}yz^{t-1} + \cdots + p_0 y + q_r z^r + \cdots + q_1 z + q_0$ in G, where $p_0, \ldots, p_{t-1}, q_0, \ldots, q_r \in k[X]$ and $0 \le t \le s$, and $-q_{t+1}$ is an inverse of f in $k[X]/(I : f^s)$.*

2. *f is a* ***zero divisor*** *in $k[X]/(I : f^s)$ if and only if $P_s \subsetneqq P_{s+1}$ and $1 \notin P_{s+1}$, i.e. $I : f^s \subsetneqq I : f^{s+1}$ and $f \notin I : f^s$.*
3. *f is* ***in the radical ideal*** *$\sqrt{I}$ if and only if there exists an integer s such that $1 \in P_s$, i.e. $I : f^s = \langle 1 \rangle$.*
4. *m is the* ***smallest*** *integer such that $I : f^\infty = I : f^m$, if and only if $P_{m-1} \subsetneqq P_m = P_s$ for all $s > m$. Further, P_m is a Gröbner bases of $I : f^\infty$.*

The above results can be applied to automatical proving of geometric theorems.

RESULTANT OF AN EQUIVARIANT POLYNOMIAL SYSTEM WITH RESPECT TO THE SYMMETRIC GROUP

Laurent Busé [1], Anna Karasoulou[2]

[1] *INRIA Sophia Antipolis-Méditeranée, France, laurent.buse@inria.fr,*
[2] *Department of Informatics & Telecommunications, National and Kapodistrian University of Athens, Greece, akarasou@di.uoa.gr*

The analysis and solving of polynomial systems are fundamental problems in computational algebra. In many applications, polynomial systems are highly structured and it is very useful to develop specific methods in order to take into account a particular structure. In this talk, we will focus on systems of n homogeneous polynomials $f_1,\ldots,f_n$ in n variables $x_1,\ldots,x_n$ that are globally invariant under the action of the symmetric group S_n of n symbols. More precisely, we will assume that for any integer $i \in \{1,2,\ldots,n\}$ and any permutation $\sigma \in S_n$

$$\sigma(f_i) := f_i(x_{\sigma(1)},x_{\sigma(2)},\ldots,x_{\sigma(n)}) = f_{\sigma(i)}(x_1,x_2,\ldots,x_n). \tag{1}$$

In the language of invariant theory these systems are called equivariant with respect to the symmetric group S_n, or simply S_n-equivariant (see for instance [5, §4] or [1, Chapter 1]). Some recent interesting developments based on Gröbner basis techniques for this kind of systems can be found in [2] with applications. In this work, we will study the resultant of these systems.

The main result of this talk is a decomposition of the resultant of a S_n-equivariant polynomial system. This formula allows to split such a resultant into several other resultants that are in principle easier to compute and that are expressed in terms of the divided differences of the input polynomial system. We emphasize that the multiplicity of each factor appearing in this decomposition is also given. Another important point of our result is that it is an exact and universal formula which is valid over the universal ring of coefficients (over the integers) of the input polynomial system. Indeed, we payed attention to use a correct and universal definition of the resultant. In this way, the formula we obtain has the correct geometric meaning and stays valid over any coefficient ring by specialization. This kind of property is particularly important for applications in the fields of number theory and arithmetic geometry where the value of the resultant is as important as its vanishing.

The discriminant of a homogeneous polynomial is also a fundamental tool in Computer Algebra. Although the discriminant of the generic homogeneous polynomial of a given degree is irreducible, for a particular class of polynomials it can be decomposed and this decomposition is always deeply connected to the geometric properties of this class of polynomials. The second main Theorem of this talk is a decomposition of the discriminant of a homogeneous symmetric polynomial. This result was actually the first goal of this work that has been inspired by the unpublished (as far as we know) note [4] by N. Perminov and S. Shakirov where a first tentative for such a formula is given without a complete proof. Another motivation was also to improve the computations of discriminants for applications in convex geometry, following a paper by J. Nie where the boundary of the cone of non-negative polynomials on an algebraic variety is studied by means of discriminants [3]. We emphasize that our formula is obtained as a byproduct of our first formula on the resultant of a S_n-equivariant polynomial system. Therefore, it inherits from the same features, namely it allows to split a discriminant into several resultants that are easier to compute and it is a universal formula where the multiplicities of the factors are provided. Here again, we payed attention to use a correct and universal definition of the discriminant.

References

[1] J.A. Dieudonné and J.B. Carrell. *Invariant theory, old and new*, Academic Press, New York-London (1971).

[2] J.-C. Faugère and J. Svartz. *Solving Polynomial Systems Globally Invariant Under an Action of the Symmetric Group and Application to the Equilibria of N vortices in the Plane*, in *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation* (ISSAC '12), pp. 170?178, NY, USA, (2012). ACM

[3] J. Nie. *Discriminants and nonnegative polynomials*, J. Symbolic Comput., 47(2) pp. 167?191, (2012).

[4] N. Perminov and S. Shakirov. Preprint arxiv:0910.5757v1. *Discriminants of Symmetric Polynomials*, (2009).

[5] P.A. Worfolk. *Zeros of equivariant vector fields: algorithms for an invariant approach*, J. Symbolic Comput., 17(6), pp. 487?511 (1994).

Symbolic Solution of Parametric Polynomial Systems with the Dixon Resultant

Robert H. Lewis

May 11, 2015

Fordham University, New York, NY 10458, USA
http://fordham.academia.edu/RobertLewis

Systems of polynomial equations with parameters arise in many fields, such as geometric computing, flexibility of molecules, chemical reactions, dynamical systems, game theory, image analysis, operations research, global positioning systems, and differential equations. In most applied problems, the best method for their symbolic solution is the Dixon-EDF resultant. We will briefly describe the method itself, then discuss problems arising from analysis of point cloud data, image processing, and other fields.

We will carefully compare Dixon-EDF to several implementations of Gröbner bases algorithms on several systems. We find that Dixon-EDF is greatly superior, often by several orders of magnitude.

Keywords: polynomial system, parameter, resultant, Dixon, determinant, symbolic computing, Gröbner basis.

Design of a Maple Package for Dixon Resultant Computation

M. Minimair[1]

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

Introduction: The Dixon resultant is a polynomial in the coefficients of $n+1$ polynomials in n variables. It vanishes if the polynomials have a common root, and therefore provides a necessary condition for the consistency of an overdetermined system of polynomial equations. Applied works, such as [1, 2], commonly use the Dixon resultant to eliminate variables from systems of polynomial equations [3], either to check consistency or to find solutions. Kapur/Saxena/Yang [4] generalized Dixon's work [5] and developed an efficient method for computing Dixon resultants of polynomials in n variables. More recently, Lewis [6] provided some heuristics to accelerate Dixon resultant computations for adequately structured polynomial systems.

Software package: The Maple package DR [7] for computing Dixon resultants includes code contributed by A. Cherba, H. Hong and M. Minimair and is maintained by Minimair. It has been extensively used by Cherba, Kapur and Minimair during past works, for example [8, 9, 10]. It includes functions for constructing Dixon matrices, computing maximal minors of matrices and various auxiliary procedures useful for applications. The design and functions of the package will be introduced and its computational efficiency will be discussed.

References

[1] E. A. Coutsias, C. Seok, M. P. Jacobson, and K. A. Dill, *A Kinematic View of Loop Closure*, J Comput Chem, **25**, pp. 510–528, (2004).

[2] B. Paláncz, *Application of Dixon resultant to satellite trajectory control by pole placement*, J. Symb. Comput., **50**, pp. 79–99, (2013).

[3] G. Nakos and R. M. Williams, *Elimination with the Dixon resultant*, Math. Educ. Res., **6**, 3, pp. 11–21, (1997).

[4] D. Kapur, T. Saxena, and L. Yang, *Algebraic and Geometric Reasoning using the Dixon Resultants*, in *Proceedings of International Symposium on Symbolic and Algebraic Computation (ISSAC), July 1994, Oxford University, England*, pp. 99–107, (1994).

[5] A. L. Dixon, *The Eliminant of Three Quantics in Two Independent Variables*, Proc Lond. Math Soc, **7**, pp. 49–69, (1908).

[6] R. H. Lewis, *Comparing acceleration techniques for the Dixon and Macaulay resultants*, Math Comput Simul, **80**, 6, pp. 1146–1152, (2010).

[7] M. Minimair, *DR: Maple package for computing Dixon projection operators (resultants)*. http://minimair.org/dr/, (2015).

[8] M. Minimair, *Randomized Detection of Extraneous Factors*, in *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, New York, NY, USA, pp. 335–342, (2014).

[9] D. Kapur and M. Minimair, *Multivariate resultants in Bernstein basis*, in *Proceedings of the 7th International Conference on Automated Deduction in Geometry*, vol. 6301 2011, Springer-Verlag, pp. 60–85, (2011).

[10] A. D. Chtcherba, D. Kapur, and M. Minimair, *Cayley–Dixon projection operator for multi-univariate composed polynomials*, J. Symb. Comput., **44**, no. 8, pp. 972–999, (2009).

Integral Bases for D-Finite Functions

M. Kauers[1], C. Koutschan[2].

[1] *Institute for Algebra, Johannes Kepler University, Linz, Austria, manuel.kauers@algebra.jku.at*

[2] *RICAM, Austrian Academy of Sciences, Linz, Austria, christoph.koutschan@ricam.oeaw.ac.at*

We propose a differential analog of the notion of integral closure of algebraic function fields. We present an algorithm for computing the integral closure of the algebra defined by a linear differential operator. Our algorithm is a direct analog of van Hoeij's algorithm for computing integral bases of algebraic function fields. This work is accepted for ISSAC'15 [1].

References

[1] M. Kauers and C. Koutschan, *Integral D-finite Functions*, Proceedings of ISSAC'15, to appear.

LINDALG: MATHEMAGIX Package for Symbolic Resolution of Linear Differential Systems with Singularities

S. S. Maddah, M. A. Barkatou

University of Limoges, XLIM, 123, Av. Albert Thomas, 87060 Limoges, France,
suzy.maddah@etu.unilim.fr, moulay.barkatou@unilim.fr

LINDALG is dedicated to the local analysis of n^{th}-order linear differential equations and first order linear differential systems. At ordinary points, it suffices to consider Taylor series (power series). Any engineering student or scientist is familiar with their resolution procedure and popular computer systems always consider a package for this goal. However, singular points require further investigation based on an analysis of a Newton polygon and matricial manipulations. Differential equations with singularities arise from countless applications and encompass a vast body of contemporary academic literature (see, e.g. [1, 7]). The package ISOLDE [4] written in the computer algebra system MAPLE is dedicated to the symbolic resolution of such systems and more generally linear functional matrix equations (e.g. difference equations).
On the other hand, the new package LINDALG [6] sets a first milestone in providing the two-decade span of ISOLDE content in an open source software. MATHEMAGIX [5] provides under GNU General Public License, a new high level general purpose language, for symbolic and certified numeric algorithms, that can be both interpreted by a shell or compiled.

References

[1] W. Balser. Formal Power Series and Linear Systems of Meromorphic Ordinary Differential Equations. *Springer-Verlag*, New York, 2000.

[2] M. Barkatou, *An Algorithm to Compute the Exponential Part of a Formal Fundamental Matrix Solution of a Linear Differential System*, Journal of App. Alg. in Eng. Comm. and Comp., 8(1), pp. 1-23 (1997).

[3] M. Barkatou, *A Rational Version of Moser's Algorithm*, in Proceedings of the International Symposium on Symbolic and Algebraic Computation, pp 297-302, ACM Press, July (1995).

[4] M. Barkatou and E. Pfluegel, ISOLDE: Integration of Systems of Ordinary Linear Differential Equations. Available at: http://isolde.sourceforge.net/

[5] J. van der Hoeven, G. Lecerf, B. Mourrain, et al. Mathemagix, 2002. Software available from *http : //www.mathemagix.org*.

[6] More information available at: *http : //www.unilim.fr/pages_perso/suzy.maddah/*

[7] W. Wasow. Asymptotic Expansions for Ordinary Differential Equations. *Dover Phoenix Editions*, 2002.

Bézout Matrices and Complex Roots of Quaternion Polynomials

Petroula Dospra[1] and Dimitrios Poulakis[2]

[1] Agricultural University of Athens,
Department of Natural Resources Management and Agricultural Engineering,
Mathematics Laboratory,
75 Iera Odos, Athens 11855, Greece
pdospra@aua.gr
[2] Aristotle University of Thessaloniki, Department of Mathematics,
Thessaloniki 54124, Greece,
poulakis@math.auth.gr

The notion of Bézout matrix is introduced by Sylvester (1853) and Cayley (1857). It is a special square matrix associated with two polynomials with very useful properties. Thus, it is an essential tool in studying broad variety of topics: zeros of polynomials, stability of differential equations, rational transformations of algebraic curves, etc. In this paper, we use Bézout matrices in order to study the complex roots of polynomials with quaternion coefficients. More precisely, quaternion polynomials have two kind of roots: isolated and spherical. A spherical root generates a class of roots which contains only one complex number z and its conjugate $\bar{z}$, and this class can be determined by z. Using Bézout matrices, we give necessary and sufficient conditions, for a quaternion polynomial to have a complex root, a spherical root, and a complex isolated root. These results are applied in the study of Rational Rotation Minimizing Frame Curves which are useful in many applications, as robotics, computer graphics, motion design and control in computer animation, swept surfaces construction etc.

Keywords: Quaternion polynomial; Bézout Matrices; Spherical Root; Isolated Root.

MCS 2010 : 12E15, 11R52, 16H05.

Nearly Optimal Bit Complexity Bounds for Computations with Structured Matrices

Elias Tsigaridas

July 6, 2015

Abstract

We present optimal, up to poly-logarithmic factors, bit complexity results for basic operations, matrix-vector multiplication and solving non-singular linear systems, with structured matrices.

LINEAR ALGEBRAIC APPROACH TO H-BASIS COMPUTATION

EROL YILMAZ

Macaulay introduced the notion of H-bases [2]. His original motivation was the transformation of systems of polynomial equations into simpler ones. The power of this concept was not really understood presumably because of the lack of facilities for symbolic computations. Later Buchberger invented Gröbner bases for computing multiplication tables for factor rings [1]. When Computer Algebra Systems came up, Buchberger's Algorithm for computing Gröbner basis is implemented to this programs. H-bases have not been used in computational problems as extensively as Gröbner basis. However, Möller and Sauer show that H-bases yield a perfect replacement for the Gröbner bases in some Numerical Analysis problems, see [([3, 4, 5])]. All approaches related to Gröbner Bases are fundamentally tied to on term orders which leads to asymmetry among the variables to be considered. On the other hand, the concept of H-bases is based solely on homogeneous terms of a polynomial. Hence H-bases lead to a significant stabilization of the computations when they used instead of Gröbner bases.

It is well known that a Gröbner basis with respect to a degree compatible ordering is an H-basis as well. However, this Gröbner basis may contain some unnecessary elements. Yılmaz and Kılıçarslan [6] gave a method of eliminating of these unnecessary elements during the Gröbner basis computation. H-basis have not been preferred over Gröbner basis because there is no general algorithm for computing it. An algorithm involving only linear algebraic computations is proposed by Moller and Thomas but it relies on the a priori knowledge of a system of generator of the syzygy module which cannot be expected to be known in advance in most situations (see [3]). The only known method for computation of a basis of syzygy module depends on Gröbner basis computation.

In this study, we give a method for computation of module of syzygies using only linear algebraic techniques. Our method computes module of syzygies only for homogeneous ideals. This is enough to give an algorithm for obtaining H-basis with only some linear algebraic and combinatorial computations when it is combined with Möller and Thomas' idea.

References

[1] B. Buchberger *An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal [in German]*, Ph. D. Thesis, University of Innsbruck, Austria 1965.

[2] F. S. Macaulay, *The Algebraic Theory of Modular Systems*, Cambridge University Press (1916).

[3] H. M. Moller and T. Sauer, *H-bases for polynomial interpolation and system solving*, Advances Comput. Math., **12** (2000), 335–362.

[4] H. M. Moller and T. Sauer, *H-bases I: The foundation*, Proceedings of Curve and Surface fitting: Saint-Malo 1999, Vanderbilt University Press (2000), 325–332.

Key words and phrases. H-bases, Gröbner bases, Syzygies.

[5] H. M. Moller and T. Sauer, *H-bases II: Applications to numerical problems*, Proceedings Curve and Surface fitting: Saint-Malo 1999, Vanderbilt University Press (2000), 333–342.

[6] E. Yılmaz and S. Kılıçarslan, *Minimal Homogeneous Basis For Polynomial Ideals*, AAECC, **15** (2004), 267–278.

Department of Mathematics, Abant İzzet Baysal University, Bolu, Turkey
E-mail address: `yilmaz_e2@ibu.edu.tr`

Computer Algebra Methods for Matrices over Rings

Session Organizers

George Labahn
University of Waterloo
glabahn@uwaterloo.ca

Qing-Wen Wang
Shanghai University
wqw@shu.edu.cn

Yang Zhang
University of Manitoba
yang.zhang@umanitoba.ca

Overview

As a research area of algebra, matrices over rings, both commutative and non-commutative, have been studied for many decades. Matrices over non-commutative rings such as quaternion and Ore algebras can be used widely in other areas like computer graphics, control theory, signal processing, physics, mechanics, and generally in solving systems of differential equations. Matrices over commutative rings, such as multivariate polynomials and power series, Dedekind domains, as well as their various projections and localizations, are also of great interest. Associative algebras are a key tool in representation theory and factorization algorithm. Some computer algebra based tools and algorithms for working with these matrices have been developed, for example, for efficient algorithms for computing Jacobson forms, Hermite forms and Popov forms for Ore matrices, and for computing Moore-Penrose inverses of quaternion matrices. Many other important problems remain open and applications unaddressed. The goal of this special session is to bring together a mixture of researchers in algebra and computer algebra to encourage exchange of ideas and stimulate new research collaborations.

Properties and applications of a simultaneous decomposition of seven matrices over real quaternion algebra

Zhuo-Heng He, Qing-Wen Wang

Shanghai University, Shanghai, P. R. China, hzh19871126@126.com (Z.H. He), wqw@staff.shu.edu.cn (Q.W. Wang)

Let H be the real quaternion algebra and $H^{n\times m}$ denote the set of all $n\times m$ matrices over H. In this paper, we construct a simultaneous decomposition of seven general real quaternion matrices with compatible sizes: $A\in H^{m\times n}, B\in H^{m\times p_1}, C\in H^{m\times p_2}, D\in H^{m\times p_3}, E\in H^{q_1\times n}, F\in H^{q_2\times n}, G\in H^{q_3\times n}$. As applications of the simultaneous matrix decomposition, we give solvability conditions, general solutions, as well as the range of ranks of the general solutions to the following two real quaternion matrix equations $BXE+CYF+DZG=A$ and $BX+WE+CYF+DZG=A$, where A,B,C,D,E,F, and G are given real quaternion matrices.

Travelling from matrices to matrix polynomials

P. Psarrakos Department of Mathematics, National Technical University, Zografou Campus 15780, Athens, GREECE, ppsarr@math.ntua.gr

The study of matrix polynomials of higher degree has attracted considerable attention in recent years. The interest has been motivated by a wide range of applications of polynomial eigenvalue problems in areas such as differential equations, systems theory, control theory, mechanics and vibrations. In this presentation, we will see how results of the standard matrix theory, concerning pseudospectra, eigenvalue condition numbers, Jordan structure, numerical ranges, (entrywise) nonnegative matrices and normality, have been extended to the setting of matrix polynomials in a natural way. In particular, basic matrix theory can be viewed as the study of the special case of matrix polynomials of first degree.

Algebraic techniques for eigenvalues of a split quaternion matrix in split quaternionic mechanics

Tongsong Jiang, Zhaozhong Zhang, Department of Mathematics, Linyi University, Linyi Shandong 276005, P. R. China, jiangtongsong@sina.com

In the study of the relation between complexified classical and non-Hermitian quantum mechanics, physicists found that there are surprising links to quaternionic and split quaternionic mechanics. The main finding is that complexified mechanical systems with real energies studied extensively in the literature over the past decade can alternatively be thought of as certain split quaternionic extensions of the underlying real mechanical systems. This identification leads to the possibility of employing algebraic techniques of quaternions and split quaternions to tackle some of the challenging open issues in complexified classical and quantum mechanics.

The eigen-problem of quaternion matrices and split quaternion matrices play important roles in the study of theories and numerical computations of quaternionic and split quaternionic mechanics. In general the following problems have hitherto remained tangential for a split quaternion matrix A in split quaternionic mechanics.

Problem 1: Does it exists right split quaternion eigenvalues for A? What is a necessary and sufficient conditions for A to have a right split quaternion eigenvalue? Problem 2: How to find all possible right split quaternion eigenvalue and corresponding split quaternion eigenvectors of A?

This paper, by means of complex representation of a split quaternion matrix, studies the eigen-problem of right split quaternion eigenvalues and corresponding split quaternion eigenvectors of a split quaternion matrix, and settles down the two problems above. It not only gives a necessary and sufficient conditions for A to have a right split quaternion eigenvalue, but also derives algebraic techniques for the right split quaternion eigenvalues and corresponding split quaternion eigenvectors of the split quaternion matrix in split quaternionic mechanics.

Algebraic methods for Least Squares problem in split quaternionic mechanics

Zhaozhong Zhang, Tongsong Jiang, Department of Mathematics, Linyi University, Linyi Shandong 276005, P. R. China, jiangtongsong@sina.com

A split quaternion(or coquaternion), which was found in 1849 by James Cockle, In the study of the relation between complexified classical and non-Hermitian quantum mechanics, physicists found that there are surprising links to quaternionic and split quaternionic mechanics. In the study of theory and numerical computations of split quaternionic mechanics, one will meet problems of approximate solutions of quaternion problems, such as approximate solutions of split quaternion linear equations $AX \approx B$ that is appropriate when there is error in the matrix B, i.e. split quaternionic least squares (SQLS) problem. In this paper, by means of complex representation and real representation of a split quaternion matrix, we study the split quaternionic least squares (SQLS) problem in two ways, and derive two algebraic techniques for finding solutions of the SQLS problem in split quaternionic mechanics. At last the examples show the effectiveness of the algebraic techniques.

MOORE-PENROSE INVERSE AND DRAZIN INVERSE OF SOME ELEMENTS IN A RING

Jianlong Chen, Department of Mathematics, Southeast University, Nanjing, 210096, China, jlchen@seu.edu.cn

In this talk, we first introduce the centralizer and give some applications to Drazin inverse, generalize some results about commutativity up to factor. Then we discuss the Drazin(resp. Moore-Penrose) invertibility of difference and product of idempotents (resp. projections). Finally we obtain some conditions on a ring such that Jacobson?s lemma is ture for Moore-Penrose inverse.(This is joint work with X.X.Zhang, H.H.Zhu, S.S.Zhang

Using Prover9 for proving some matrix equations

R. Padmanabhan, Yang Zhang, Department of Mathematics, University of Manitoba, Winnipeg, MB, R3T 2N2, Canada,
{padman, zhang39}@cc.umanitoba.ca

In this talk, we will introduce how to Prover9 to prove some matrix equations. In particular, some equations regarding generalized inverses and Moore-Penrose inverses of matrices.

Some results concerning condensed Cramer's rule for the general solution to some restricted quaternion matrix equations

Guang-Jing Song, School of Mathematics and Information Sciences, Weifang University Weifang 261061, P.R. China, songguangjing2005@163.com

In this paper, we aim to consider the condensed Cramer's rules for the general solution, the least square solution and the least norm solution of

$$AXB = C, \;\; R_r(X) \subseteq T_1, \;\; N_r(X) \supseteq S_1 \tag{1}$$

$$AXB = C, \;\; R_l(X) \subseteq T_2, \; N_r(X) \supseteq S_2, \tag{2}$$

respectively. We start with some basic concepts and results about the row and column determinants of a square matrix over the quaternion skew field. And then, when (1) and (2) are consistent, we derive the condensed Cramer's rules for the unique solution and the general solution, respectively. As applications, we give the determental expressions of $A^{(1,3)}$ and $A^{(1,4)}$, respectively. Moreover, we show a set of Cramer's rules for the least squares solution, the least norm solution as well as the best approximate solution of the restricted quaternion matrix equation (1) and (2), respectively. Some results are even new for the complex matrix cases. At last, we show a numerical example to illustrate the main results.

Inertia of weighted graphs

Guihai Yu, Shandong Institute of Business and Technology, and Nankai University, China, yuguihai@126.com

Let G_w be a weighted graph. The inertia of G_w is the triple $In(G_w) = \big(i_+(G_w), i_-(G_w), i_0(G_w)\big)$, where $i_+(G_w), i_-(G_w), i_0(G_w)$ are the number of the positive, negative and zero eigenvalues of the adjacency matrix $A(G_w)$ of G_w including their multiplicities, respectively. $i_+(G_w)$, $i_-(G_w)$ is called the *positive, negative index of inertia* of G_w, respectively. In this report we present a lower bound for the positive, negative index of weighted unicyclic graphs of order n with fixed girth and characterize all weighted unicyclic graphs attaining this lower bound. Moreover, we characterize the weighted unicyclic graphs of order n with two positive, two negative and at least $n-6$ zero eigenvalues, respectively.

More on minmum skew-rank of graphs

Hui Qu, Shandong Institute of Business and Technology

The minimum (maximum) skew-rank of a simple graph G over real field is the smallest (largest) possible rank among all skew-symmetric matrices over real field whose ij-th entry is nonzero whenever v_iv_j is an edge in G and is zero otherwise. In this report we list some properties of minimum skew-rank of graphs and present a lower (upper) bound for minimum (maximum) skew-rank of unicyclic graph of order n with girth k, characterize unicyclic graphs attaining the extremal values. Moreover, we characterize the unicyclic graphs by which the skew-symmetric matrices described are nonsingular.

Post-Lie algebra structures on solvable Lie algebrat $t(2,C)$

Xiaomin Tang, Department of Mathematics, Heilongjiang University, Harbin,
150080, PR China, x.m.tang@163.com

The post-Liealgebra is an enriched structure of the Lie alge-bra introduced by Vallette. In this paper we give a complete classification of post-Liealgebra structures on solvable Lie algebra $t(2,C)$, the Lie algebra of 2×2 upper triangular matrices. Using Groebner basis package in computer algebra software Maple, we give all 65 types of these post-Lie algebra structures. Furthermore, we discuss their isomorphism classes and obtain one necessary and sufficient condition.

Open Source Software and Computer Algebra

Session Organizer

Razvan A. Mezei
Lenoir-Rhyne University
razvan.mezei@lr.edu

Overview

This session aims to bring together researchers and educators from all fields related to Computer Algebra as well as the use of Free Open Source Software. It aims at providing a stimulating forum where experts in these fields will be able to share their experiences with the use of free open source software for their computations. The participants will get to discuss the advantages and disadvantages of using these types of systems. As an ice-breaker we'll have a look at what Sage Math can provide to Algebra, Calculus, and Numerical Analysis (among others).

Implementation of Coefficient-Parameter Homotopies in Parallel

Daniel J. Bates[1], Daniel Brake[2], Matthew Niemerg[3]

[1] *Colorado State University, Fort Collins, CO bates@math.colostate.edu*
[2] *Notre Dame University, South Bend, IN brake@nd.edu*
[3] *Fields Institute, Toronto, Canada research@matthewniemerg.com*

Solving polynomial systems is a problem ubiquitous in the sciences. Often, scientists and engineers are interested in solving the same polynomial system but with different coefficient values. The coefficient-parameter homotopy in parallel is a highly effective technique to accomplish this task and is implemented in the open-source software package `paramotopy`. We describe several key features of this software and give some examples of applications in the sciences and engineering.

The Four Corner Magic and semi pandiagonal Squares

S. Al-Ashhab[1]

[1] *Al-Albayt University, Jordan (ahhab@aabu.edu.jo),*

In this paper we consider the old famous problem of magic squares. A semi magic square is a square matrix, where the sum of all entries in each column or row yields the same number. Some authors call it magic square. This number is called the magic constant. We call a semi magic square a magic square if both main diagonals sum up to the magic constant. A natural magic square of order n is a matrix of size $n \times n$ such that its entries consist of all integers from one to n^2. The magic constant in this case is

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

A pandiagonal magic square is a magic square such that the sum of all entries in all bent-diagonals equals the magic constant. A symmetric magic square is a natural magic square of order n such that the sum of all opposite entries equals $n+1$.

Example A natural symmetric magic square

$$\begin{bmatrix} 15 & 14 & 1 & 18 & 17 \\ 19 & 16 & 3 & 21 & 6 \\ 2 & 22 & 13 & 4 & 24 \\ 20 & 5 & 23 & 10 & 7 \\ 9 & 8 & 25 & 12 & 11 \end{bmatrix}$$

If the two main diagonals sum to the magic constant then the square is called a magic square. An off-diagonal is a combination of two parallel diagonal lines to the same main diagonal. The two parallel diagonal lines must occur on opposite sides of the main diagonal and they can only be combined if the combination has the same number of entries as the main diagonal. Two examples of an off-diagonal line are 13, 7, 4, 10 and 1, 7, 16, 10 as shown in Figure 2. There are 3 off-diagonals corresponding to each main diagonal. A pandiagonal square is a magic square where all off-diagonals sum to the magic constant.

Example A natural pandiagonal magic square

$$\begin{bmatrix} 1 & 8 & 13 & 12 \\ 14 & 11 & 2 & 7 \\ 4 & 5 & 16 & 9 \\ 15 & 10 & 3 & 6 \end{bmatrix}$$

The number of natural magic squares of order five is known. It is well-known that there are pandiagonal magic squares and symmetric squares of order five. The number of natural magic squares of order six is til now unknown. We give here the number of a subset of such squares. It is well-known that there are no pandiagonal magic squares nor symmetric squares of order six. We define here classes of magic squares of order six, which satisfy some of the conditions for both types. It is well-known that there are pandiagonal and symmetric magic squares of order seven.

Example A natural pandiagonal and symmetric magic square

$$\begin{bmatrix} 1 & 39 & 34 & 21 & 35 & 8 & 37 \\ 27 & 9 & 12 & 36 & 24 & 19 & 48 \\ 40 & 30 & 17 & 46 & 7 & 32 & 3 \\ 45 & 6 & 28 & 25 & 22 & 44 & 5 \\ 47 & 18 & 43 & 4 & 33 & 20 & 10 \\ 2 & 31 & 26 & 14 & 38 & 41 & 23 \\ 13 & 42 & 15 & 29 & 16 & 11 & 49 \end{bmatrix}$$

We focus in this paper on the following kind of magic squares:

Four corner magic squares 6 by 6

A four corner magic square of order 6 is magic square $(a_{ij})_{\substack{i=1,\dots,6\\ j=1,\dots,6}}$ with magic constant $3s$ such that

$$a_{ij} + a_{(i+3)(j+3)} + a_{i(j+3)} + a_{(i+3)j} = 2s$$

holds for each $i = 1,2,3$ and $j = 1,2,3$ and

$$a_{33} + a_{44} + a_{34} + a_{43} = 2s.$$

The entries of a four corner magic square of order 6 satisfy

$$a_{14} + a_{25} + a_{36} + a_{41} + a_{52} + a_{63} = 3s,\ a_{13} + a_{22} + a_{31} + a_{61} + a_{55} + a_{64} = 3s$$

These two conditions represent the sum of the entries of two broken diagonals. If the magic square is pandiagonal, then we have to consider all broken diagonals. To see the validity of the first equation we know from the definition that

$$a_{11} + a_{44} + a_{14} + a_{41} = 2s, a_{22} + a_{55} + a_{25} + a_{52} = 2s, a_{33} + a_{66} + a_{36} + a_{63} = 2s$$

hold. Adding up these equations and subtracting from them the following equation

$$a_{11}+a_{22}+a_{33}+a_{44}+a_{55}+a_{66}=3s$$

yields the desired equation. A four corner magic square is said to have symmetric center if $a_{33}+a_{44}=s$ and $a_{34}+a_{43}=s$. A four corner magic square is said to have symmetric center if $a_{33}+a_{34}=s$ and $a_{43}+a_{44}=s$. A four corner magic square is said to have positive determinat center if $a_{33}a_{44}-a_{34}a_{43}>0$. A four corner magic square is said to have negative determinat center if $a_{33}a_{44}-a_{34}a_{43}<0$. A four corner magic squares with symmetric center is a four corner magic square of order 6 can be written as

$$\begin{bmatrix} x & f & g & t & G & M \\ z & h & n & j & q & N \\ w & E & e & a & m & D \\ A & k & s-a & s-e & H & R \\ 2s-o-j-z & p & d & o & 2s-p-q-h & T \\ B & F & W & J & L & p+q-x \end{bmatrix}$$

where

$$\begin{gathered} A=s-t-x+e, B=j+o+t-w-e, \\ D=d-a+g+n-p-q+x, \\ E=3s-e-a-m-w-D, \\ F=3s-f-h-k-p-E, \\ G=j-g-f+o+p+q+s-w-x-e, \\ H=g-j-k-o-p-q+s+w+x+e, \\ J=2s-j-o-a-t+e, \\ M=3s-f-g-t-x-G, \\ N=3s-j-n-q-h-z, \\ L=f+h+k-m+p-s, \\ R=s+a+e-k-A-H, \\ T=h-d+j+q-s+z, \\ W=a-d-g-n+2s-e. \end{gathered}$$

We see that it has seventeen independent variables. This formula was computed by maple.

Property preserving transformations

There are seven classical transformations, which take a magic square into another magic square. They are the combinations of the rotations with angles $\frac{\pi}{2},\pi,\frac{3\pi}{2}$ and transpose operation. Now, a four corner magic squares with symmetric center can be transformed as follows into another one of the same kind: we make these interchanges simultaneously: interchange a_{12} (res. a_{62}) with a_{15} (res. a_{65}), interchange a_{21} (res. a_{26}) with a_{51} (res. a_{56}), interchange a_{22} (res. a_{55}) with a_{25} (res. a_{52}), interchange a_{23} (res. a_{24}) with a_{53} (res. a_{54}), interchange a_{32} (res. a_{42}) with a_{35} (res. a_{45}).

We can use this transformation to reduce the number of computed natural magic squares. In order to eliminate the effect of the previous transformations we compute all natural four corner magic squares for which the following conditions hold:

$$a_{52} < a_{25}, a_{34} < a_{33} < a_{44}.$$

When we calculate the number of all natural squares, we multiply then the number with sixteen.

Enumertaion of squares

In the papers [2], [3] and [4] there is an enumertaion of subsets of such squares. There are 232 centers of the natural positive determinant four corner magic squares. According to [3] there are

$$30350772825 * 16 = 485612365200$$

different squares of this type. There are 153 possible symmetric centers of the natural four corner magic squares. According to [2] there are

$$28634584244 * 16 = 458153347904$$

different natural four corner magic squares associated with symmetric center. There are 306 possible semi symmetric centers of the natural four corner magic squares. According to [4] there are

$$101425060998 * 16 = 1622800975968$$

different natural four corner magic squares associated with semi symmetric center. In this paper we present the last list in the problem of counting the number of counting four corner magic squares. In the following list we see the number of squares with negative detrminant, whose center are neither symmetric or semi symmetric:

a	Centers	number	a	Centers	number
1	255	38523022675	9	183	24126017814
2	270	40662919383	10	152	17629237298
3	279	39628193947	11	121	15244199949
4	282	40866368479	12	87	11061888729
5	280	39666915624	13	55	7037768734
6	266	37157828666	14	33	4328085633
7	242	33133901727	15	15	2059934349
8	214	27807342954	16	4	618706214

Hence, there are

$$8639404003872$$

different four corner magic squares of order six. By comparing all calculated values we see that the maximum number of squares associated with a fixed center is the number generated by the center $a = 17, b = 20, e = 18$, namely 398369256. Further, the minimum number of squares associated with a fixed center is the number generated by the center $a = 1, b = 35, e = 2$, namely 80012582.

Semi pandiagonal magic squares

We can generalize the concept of four corner magic square to the semi pandiagonal magic square. It has the following structure

$$\begin{bmatrix} a & D & c & d & f & H \\ h & 2s-o-m-e & k & l & m & E \\ A & r & u & v & J & I \\ q & p & z & 2s-u-v-z & y & L \\ n & o & i & x & e & 3s-o-i-n-x-e \\ B & F & M & N & G & Y \end{bmatrix}$$

where

$$\begin{gathered} A = d-c+l+m+o+p+q-s-2u-v+x+y-z, \\ B = 3s-a-h-q-n-A, \\ D = 4s-2d-f-h-l-n-p-2q-2a+2u+2v-x-y+2z, \\ E = o-k-l-h+s+e, \\ F = 2a+2d+f+h+l+m+n+2q-r-3s-2u-2v+x+y-2z+e, \\ G = k-f+l-m+p+r+i-s+x-e, \\ H = 3s-a-c-d-f-D, \\ I = c-d+k-m-o-q+i+u+z, \\ J = 4s-l-p-r-i-k-x-y, \end{gathered}$$

$$\begin{aligned}L &= s-q-p+u+v-y,\\ M &= 3s-k-i-c-u-z,\\ N &= s-l-d+u-x+z,\\ Y &= m-a+o-s+v+z.\end{aligned}$$

It is worth mentioning that the two dependent variables in the frame of center square (E and H) depends only on the variables in the outer frame. This is helpful by programming in order to reduce run time. The problem of counting the natural squares of this type of squares is yet unsolved.

Symbolic computations of the determinant

It is sometimes of interest to determine the determinant of the magic square as a square matrix. In the case of the semi pandiagonal magic squares there are cases when the deter-minant is zero. In general the determinant is not zero for any semi pandiagonal magic square. In case we have all entries of the frame of outer 4 by 4 center (E, k, l, m, r, H, p, y, o and e) as the value

$$\frac{s}{2}$$

Then, we can prove using symbolic (maple) calculation software that the determinant is zero. In general any square of the following structure has this property:

$$\begin{bmatrix} a & x & c & d & f & t \\ h & \frac{s}{2} & \frac{s}{2} & \frac{s}{2} & \frac{s}{2} & s-h \\ o & \frac{s}{2} & u & v & \frac{s}{2} & n \\ q & \frac{s}{2} & z & 2s-u-v-z & \frac{s}{2} & w \\ n & \frac{s}{2} & \frac{s}{2} & \frac{s}{2} & \frac{s}{2} & s-n \\ l & y & m & p & g & r \end{bmatrix}$$

References

[1] S. Al-Ashhab, *Magic Squares 5x5*, the international journal of applied science and computations, Vol. 15, No.1, pp. 53-64 (2008).

[2] S. Al-Ashhab, *Even-order Magic Squares with Special Properties*, International Journal of Open Problems in Mathematics and Computer Science, Vol. 5, No. 2 (2012).

[3] S. Al-Ashhab, *Special Magic Squares of Order Six*, Research Open Journal of Information Science and Application, Vol. 1, No. 1 , pp 01-19 (August 2013).

[4] S. Al-Ashhab, *Special Magic Squares of Order Six and Eight*, International Journal of Digital Information and Wireless Communications (IJDIWC) 1(4): 769-781 (2012).

[5] S. Al-Ashhab, *Negative four corner magic squares of Order Six with a Between 1 and 5*, Qatar Foundation Annual Research Conference (ARC 2014 conference).

[6] S. Al-Ashhab, *The Number of Four Corner Magic Squares of Order Six*, British Journal of Applied Science Technology 7(2): 141-155, 2015, Article no. BJAST. 2015. 132.

[7] J. Bellew, *Counting the Number of Compound and Nasik Magic Squares*, Mathematics Today, pp. 111-118, (1997).

Use computer algebra system Piranha for expansion of the Hamiltonian and construction averaging motion equations of the planetary system problem

A.S. Perminov, E.D. Kuznetsov

Ural Federal University, Ekaterinburg, Russia, perminov12@yandex.ru, eduard.kuznetsov@urfu.ru

Work is related to the problem of planetary system dynamical evolution. Hamiltonian expansion into the Poisson series and construction of averaging motion equations by Hori-Depri method are considered. Calculations performed by means of computer algebra system Piranha [1] which is echeloned Poisson series processor. It is new developing C++ code with Python interface for analitical calculations with polynomials and Poisson series.

Hamiltonian is written in Jacobi coordinates with using second system Poincare elements. It allows simplifying an angular part of series. In this case only one angular element – mean longitude, is defined. Use of celestial mechanics special functions, such as Legendre polynomials, allows substantially reducing of number expansion terms, necessary working memory and disk space. We have implemented a set of Python functions for construction of classical celestial mechanics expansions, such as x/a, y/a, z/a, a/r, r/a, $1/\Delta$ and others, in Poincare elements. By integrating an angular part of Hamiltonian and using Poisson brackets we can get averaging motion equations for a planetary system.

The expansion of Hamiltonian is constructed up to 11 degree of Poincare elements and third degree of small parameter. It allows get high precision motion equations for Solar system and various extrasolar systems also. The algorithm of expansion into the Poisson series and construction of motion equations is presented in this work.

References

[1] F. Biscani, *The Piranha computer algebra system.* https://github.com/bluescarni/piranha (2015).

Use of Linux Open-Source Software and Maple in Analyzing the New Goeken-Johnson Runge-Kutta Type Methods

Adrian Ionescu[1], Rea Ulaj[2]

[1] *Wagner College, US, ionescu@wagner.edu*
[2] *Wagner College, US, rea.ulaj@wagner.edu*

The autonomous ordinary differential equation IVP

$$\begin{aligned} y' &= f(y), \quad y \in \mathbf{R^n}, \\ y(x_0) &= y_0, \quad x_0 \in R,\, y_0 \in \mathbf{R^n}, \end{aligned}$$

are traditionally solved numerically by using the Runge-Kutta methods. At the core of the Runge-Kutta methods are the evaluations of $f(y)$.

In [1], [2], some new Runge-Kutta methods have been developed, in which the user will evaluate both f and f_y. The novel feature of this approach is the replacement of evaluations of f by approximations or evaluations of f_y.

We have implemented the Goeken-Johnson algorithms in [3], by using C. In this presentation, we compare the classical Runge-Kutta methods of orders 3, 4 and 5, and the corresponding new Goeken-Johnson methods using approximations of both f and f_y, by using open-source software (Linux) and Maple for f_y. These results indicate that the new methods are at least comparable if not better than the classical methods. We have also implemented a new Goeken-Johnson-type interpolation method based on an algorithm in [4] and we have a complete analysis comparing the advantages of each method by using Linux open-source software and Maple.

References

[1] D. Goeken and O. Johnson, *Fifth-Order Runge-Kutta with Higher Order Derivative Approximations,* Electronic Journal of Differential Equations Conference 02, 1999, pp 1-9.

[2] D. Goeken and O. Johnson, Runge-Kutta with Higher Order Derivative Approximations, *Applied Numerical Mathematics,* **34**, 207-218, 2000.

[3] A. Ionescu, O. Johnson. C Software for Some New Autonomous Methods, *WSEAS Multiconference (AIC, ISTASC, ISCGAV),* Vouliagmeni, Greece, August 24-26, 2007

[4] W.H. PRESS, S.A. TEUKOLSKY, W.T. VETTERLING and B.P. FLANNARY. *Numerical Recipes in C,* Cambridge University Press, New York, 1997.

Use of Linux Open-Source Software and Maple in Analyzing the New Goeken-Johnson Runge-Kutta Type Methods

Adrian Ionescu[1], Rea Ulaj[2]

[1] *Wagner College, US, ionescu@wagner.edu*
[2] *Wagner College, US, rea.ulaj@wagner.edu*

The autonomous ordinary differential equation IVP

$$\begin{aligned} y' &= f(y), \quad y \in \mathbf{R^n}, \\ y(x_0) &= y_0, \quad x_0 \in R,\, y_0 \in \mathbf{R^n}, \end{aligned}$$

are traditionally solved numerically by using the Runge-Kutta methods. At the core of the Runge-Kutta methods are the evaluations of $f(y)$.

In [1], [2], some new Runge-Kutta methods have been developed, in which the user will evaluate both f and f_y. The novel feature of this approach is the replacement of evaluations of f by approximations or evaluations of f_y.

We have implemented the Goeken-Johnson algorithms in [3], by using C. In this presentation, we compare the classical Runge-Kutta methods of orders 3, 4 and 5, and the corresponding new Goeken-Johnson methods using approximations of both f and f_y, by using open-source software (Linux) and Maple for f_y. These results indicate that the new methods are at least comparable if not better than the classical methods. We have also implemented a new Goeken-Johnson-type interpolation method based on an algorithm in [4] and we have a complete analysis comparing the advantages of each method by using Linux open-source software and Maple.

References

[1] D. Goeken and O. Johnson, *Fifth-Order Runge-Kutta with Higher Order Derivative Approximations,* Electronic Journal of Differential Equations Conference 02, 1999, pp 1-9.

[2] D. Goeken and O. Johnson, Runge-Kutta with Higher Order Derivative Approximations, *Applied Numerical Mathematics,* **34**, 207-218, 2000.

[3] A. Ionescu, O. Johnson. C Software for Some New Autonomous Methods, *WSEAS Multiconference (AIC, ISTASC, ISCGAV),* Vouliagmeni, Greece, August 24-26, 2007

[4] W.H. PRESS, S.A. TEUKOLSKY, W.T. VETTERLING and B.P. FLANNARY. *Numerical Recipes in C,* Cambridge University Press, New York, 1997.

Index