Russian Academy of Sciences
St.Petersburg Department
of Steklov Mathematical Institute
Euler International Mathematical Institute
St.Petersburg Electrotechnical University "LETI"

International Conference

Polynomial Computer Algebra

International Conference on Polynomial Computer Algebra

St. Petersburg, April, 2018

Санкт Петербург
2018

ISBN 978-5-9651-1141-1

International Conference
Polynomial Computer Algebra '2018
St. Petersburg, Russia
April 16-21, 2018
International Euler Institute

International Conference Polynomial Computer Algebra '2016; St. Petersburg, April 18-21 2018/ Euler International Mathematical Institute, Ed. by N.N.Vassiliev, VVM Pubishing, 2018, 121 p.

The book contains short papers, extended abstracts and abstracts of reports presented at the International Conference on Polynomial Computer Algebra 2018, St.Petersburg, April 2018

Agenda

April 16

9:30 – 10:20	**Registration, coffee**
10:20 – 10:30	**Opening the conference**
10:30 – 11:10	**Vladimir Gerdt, Markus Lange-Hegermann, Daniel Robertz** Thomas decomposition of differential systems andits implementation in Maple
11:10 – 11:40	**Vladimir Kornyak** Irreducible Decomposition of Representations of Finite Groups via Polynomial Computer Algebra
11:40 – 12:00	**Coffee break**
12:00 – 12:30	**Ronen Peretz** A sharp version of Shimizu's theorem on entire automorphic functions
12:30 – 13:00	**Nikolai Proskurin** Notes on character sums and complex functions over finite fields
13:00 – 15:00	**Lunch**
15:00 – 15:30	**Evgenii Mityushov, Natalia Misyura, Svetlana Berestova** On finite subgroups of SO(3), regular polyhedrons in R4 and the spherical motion of rigid body
15:30 – 16:00	**Alexandr Seliverstov** Real cubic hypersurfaces containing no line of singular points
16:00 – 16:30	**Coffee break**
16:30 – 17:00	**Mikhail Babich, Sergey Slavyanov** Links between second-order Fuchsian equations and first-order linear systems
17:00 – 17:30	**Aleksandr Salatich, Sergey Slavyanov** Confluent Heun Equation and equivalent first-order systems
17:30 – 18:00	**Maksim Karev** Double Hurwitz Numbers
18:30	**WELCOME PARTY**

April 17

10:00 – 10:50	**Lorenzo Robbiano** Computational Linear and Commutative Algebra
10:50 – 11:20	**Coffee break**
11:20 – 12:10	**Chenqi Mou** On the chordality of polynomial sets in triangular decomposition in top-down style
12:10 – 13:00	**Dima Grigoriev, Nicolai Vorobjov** Upper bounds on Betti numbers of tropical prevarieties
13:00 – 15:00	**Lunch**
15:00 – 15:20	**Sergei Soloviev, Mark Spivakovsky, Nikolay Vassiliev** To the memory of Sergei Baranov
15:20 – 16:10	**Anatoly Vershik** To make simulation on algorithm RSK for Bernoulli sequences
16:10 – 16:40	**Coffee break**
16:40 – 17:10	**Mikhail Malykh, Leonid Sevastianov, Yu Ying** Elliptic functions and finite difference method
17:10 – 17:40	**Andrei Malyutin** What does a random knot look like?
17:40 – 18:10	**Vahagn Abgaryan, Arsen Khvedelidze, Astghik Torosyan** On a moduli space of the Wigner quasiprobability distributions

April 18

10:00 – 10:50	**Michela Ceria, Teo Mora** Combinatorics of ideals of points: a Cerlienco-Mureddu- like approach for an iterative lex game.
10:50 – 11:20	**Alexander Chistov** A New Approach to Effective Computation of the Dimension of an Algebraic Variety
11:20 – 11:50	**Coffee break**
11:50 – 12:30	**Martin Kreuzer, Le Ngoc Long, Lorenzo Robbiano** On the Cayley-Bacharach Property

12:30 – 13:00	**Alexander Batkhin** q-Analogue of discriminant set and its computation
13:00 – 15:00	**Lunch**
15:00 – 15:30	**Dominik Michels, Vladimir Gerdt, Dmitry Lyakhov, Yuri Blinkov** On Strongly Consistent Finite Difference Approximations
15:30 – 16:00	**Aleksandr Mylläri, Tatiana Mylläri, Anna Myullyari, Nikolay Vassiliev** On the complexity of trajectories in the equal-mass free-fall three-body problem
16:00 – 16:30	**Alexander Tiskin** Weighted seaweed braids
16:30 – 17:00	**Coffee break**
17:00 – 17:30	**Darya Chemkaeva, Alexander Flegontov** Bifurcation diagrams for polynomial nonlinear ODE
17:30 – 18:00	**Ioannis Parasidis, Efthimios Providas** Factorization Method for the Second-Order LinearNonlocal Difference Equations
18:30	**Chamber music Concert. Euler Institute**

April 19

10:00 – 10:40	**Mark Spivakovsky** On the Pierce-Birkhoff conjecture and related problems.
10:40 – 11:20	**David R. Stoutemyer, David J. Jeffrey, Robert M.Corless** Integration and the specialization problem
11:20 – 11:50	**Coffee break**
11:50 – 12:30	**Nikolai Vavilov** Reverse decomposition of unipotents
12:30 – 14:00	**Lunch**
14:00	**Bus Excursion around St.Petersburg** **The bus will start from the Andersen hotel at 14:00.**
19:00	**BANQUET**

April 20

10:00 – 10:40	**Fedor Petrov** Arithmetic progressions in 2-groups
10:40 – 11:10	**Vasilii Duzhin, Nikolay Vassiliev** Schutzenberger transformation on graded graphs: Implementation and numerical experiments.
11:10 – 11:40	**Coffee break**
11:40 – 12:10	**Anton Chukhnov, Ilya Posov, Sergei Pozdniakov** Computer assisted constructive tasks as tasks with infinite set of solutions for math olympiads and contests
12:10 – 12:40	**Victor Edneral, Valery Romanovski** Local and Global Integrability of ODEs
12:40 – 14:30	**Lunch**
14:30 – 15:00	**Semjon Adlaj** Back to solving the quintic, depression and Galois primes
15:00 – 15:30	**Dmitry Pavlov** Usage of Automatic Differentiation in Some Practical Problems of Celestial Mechanics
15:30 – 16:00	**Dan Aksim, Dmitry Pavlov** On the Extension of Adams–Bashforth–Moulton Methods for Numerical Integration of Delay Differential Equations and Application to the Moon's Orbit
16:00 – 17:00	**Free round table discussion, Closing of the Conference, coffee**

Table of content

Vahagn Abgaryan, Arsen Khvedelidze, Astghik Torosyan
On a moduli space of the Wigner quasiprobability distributions 10

Semjon Adlaj
Back to solving the quintic, depression and Galois primes 12

Dan Aksim, Dmitry Pavlov
On the Extension of Adams–Bashforth–Moulton Methods for Numerical Integration of Delay Differential Equations and Application to the Moon's Orbit 17

Mikhail Babich, Sergey Slavyanov
Links between second-order Fuchsian equations and first-order linear systems 18

Alexander Batkhin
q-Analogue of discriminant set and its computation 20

Michela Ceria, Teo Mora
Combinatorics of ideals of points: a Cerlienco-Mureddu- like approach for an iterative lex game. 25

Darya Chemkaeva, Alexander Flegontov
Bifurcation diagrams for polynomial nonlinear ODE 29

Alexander Chistov
A New Approach to Effective Computation of the Dimension of an Algebraic Variety 36

Anton Chukhnov, Ilya Posov, Sergei Pozdniakov
Computer assisted constructive tasks as tasks with infinite set of solutions for math olympiads and contests 39

Vasilii Duzhin, Nikolay Vassiliev
Schutzenberger transformation on graded graphs: Implementation and numerical experiments. 41

Victor Edneral, Valery Romanovski
Local and Global Integrability of ODEs 47

Vladimir Gerdt, Markus Lange-Hegermann, Daniel Robertz
Thomas decomposition of differential systems andits implementation in Maple 52

Dima Grigoriev, Nicolai Vorobjov
Upper bounds on Betti numbers of tropical prevarieties 54

Maksim Karev
Double Hurwitz Numbers 55

Vladimir Kornyak
Irreducible Decomposition of Representations of Finite Groups via Polynomial Computer Algebra 57

Martin Kreuzer, Le Ngoc Long, Lorenzo Robbiano
On the Cayley-Bacharach Property 62

Mikhail Malykh, Leonid Sevastianov, Yu Ying
Elliptic functions and finite difference method 66

Andrei Malyutin
What does a random knot look like? 69

Dominik Michels, Vladimir Gerdt, Dmitry Lyakhov, Yuri Blinkov
On Strongly Consistent Finite Difference Approximations 72

Evgenii Mityushov, Natalia Misyura, Svetlana Berestova
On finite subgroups of SO(3), regular polyhedrons in R4 and the spherical motion of rigid body 76

Chenqi Mou
On the chordality of polynomial sets in triangular decomposition in top-down style 78

Aleksandr Mylläri, Tatiana Mylläri, Anna Myullyari, Nikolay Vassiliev
On the complexity of trajectories in the equal-mass free-fall three-body problem 82

Ioannis Parasidis, Efthimios Providas
Factorization Method for the Second-Order LinearNonlocal Difference Equations 85

Dmitry Pavlov
Usage of Automatic Differentiation in Some Practical Problems of Celestial Mechanics 90

Ronen Peretz
A sharp version of Shimizu's theorem on entire automorphic functions 91

Fedor Petrov
Arithmetic progressions in 2-groups 96

Nikolai Proskurin
Notes on character sums and complex functions over finite fields 97

Lorenzo Robbiano
Computational Linear and Commutative Algebra 104

Aleksandr Salatich, Sergey Slavyanov
Confluent Heun Equation and equivalent first-order systems 105

Alexandr Seliverstov
Real cubic hypersurfaces containing no line of singular points 109

Mark Spivakovsky
On the Pierce-Birkhoff conjecture and related problems. 111

David R. Stoutemyer, David J. Jeffrey, Robert M.Corless
Integration and the specialization problem 113

Alexander Tiskin
Weighted seaweed braids 118

Nikolai Vavilov
Reverse decomposition of unipotents 119

On a moduli space of the Wigner quasiprobability distributions

Vahagn Abgaryan, Arsen Khvedelidze and Astghik Torosyan

Nowadays, due to the quantum engineering needs, a long-standing problem of finding "quantum analogues" for the statistical distributions of classical systems became an actual again. Mathematically this issue can be formulated as a problem of finding the mapping between operators on the Hilbert space of a finite-dimensional quantum system and the Wigner quasiprobability distributions [1] defined over the symplectic flag manifold [2, 3]. Based on the postulates known as the Weyl-Stratonovich correspondence [4, 5], the Wigner quasiprobability distribution for a generic N-level quantum system can be constructed from two objects: the density matrix ϱ describing a quantum state, and the so-called Stratonovich-Weyl kernel $\Delta(\Omega_N)$ defined over the symplectic manifold Ω_N. According to our recent study [3], the eigenvalues of the kernel $\Delta(\Omega_N)$ satisfy the set of algebraic equations. In present report an ambiguity in the solution to those "master equations" will be analyzed and the corresponding moduli space of the Wigner quasiprobability distribution will be determined. The general consideration will be exemplified by a detailed description of the Wigner quasiprobability distributions of 2, 3 and 4-dimensional systems.

References

[1] E.P.Wigner, *On the quantum correction for thermodynamic equilibrium*, Phys.Rev **40** 749-759, 1932

[2] C.Briff and A. Mann, *Phase-space formulation of quantum mechanics and quantum-state reconstruction for physical systems with Lie-group symmetries*, Phys.Rev. **59**, 971, 1999.

[3] A.Khvedelidze and V.Abgaryan, *On the Family of Wigner Functions for $\boldsymbol{N}$-Level Quantum System*, arXiv: https://arxiv.org/abs/1708.05981, 2018.

[4] H.Weyl *Gruppentheorie und Quantenmechanik* (Hirzel-Verlag, Leipzig), 1928.

[5] R.L.Stratonovich, *On distributions in representation space*, Soviet Physics JETP **4**, 6, 891-898, 1957.

Vahagn Abgaryan
Laboratory of Information Technologies
Joint Institute for Nuclear Research
141980 Dubna, Russia
e-mail: vahagnab@googlemail.com

Arsen Khvedelidze
A Razmadze Mathematical Institute
Iv. Javakhishvili, Tbilisi State University
Tbilisi, Georgia
Institute of Quantum Physics and Engineering Technologies
Georgian Technical University
Tbilisi, Georgia
National Research Nuclear University
MEPhI (Moscow Engineering Physics Institute)
115409 Moscow, Russia
Laboratory of Information Technologies
Joint Institute for Nuclear Research
141980 Dubna, Russia
e-mail: akhved@jinr.ru

Astghik Torosyan
Laboratory of Information Technologies
Joint Institute for Nuclear Research
141980 Dubna, Russia
e-mail: astghik@jinr.ru

Back to solving the quintic, depression and Galois primes

Semjon Adlaj

Abstract. Évariste Galois is best known for proving the insolubility of the general quintic via radicals. There, he (merely) confirmed the ingenious insights of Carl Gauss, Paolo Ruffini and Niels Abel. Yet, Galois went on (spectacularly alone) to formulate both necessary and sufficient criterion for solubility of a general algebraic equation via radicals. Even more, he was undeniably the first to actually solve the general quintic via exhibiting it as a modular equation of level 5. We aim and (hopefully) succeed at lifting any remaining doubts, concerning the latter (persistently hardly ever known) claim. And along with presenting Galois construction for depressing the degree of the modular equation of level 5, 7 or 11, we show that such construction is unique for the (Galois) prime 5, but one more construction is possible for each of the two remaining Galois primes 7 and 11.

In his last letter [5], eloquently described by Hermann Weyl as "the most substantial piece of writing in the whole literature of mankind", Évariste Galois indicated sufficient and necessary condition for depressing the degree of the modular equation of prime level. For this purpose he introduced the projective special linear group over a prime field, which we denote by G_p,[1] and observed that it was simple whenever the prime p strictly exceeded the prime 3.[2] He pointed out the three exceptional primes for which the group G_p possessed a subgroup of index, coinciding with p. These were the primes 5, 7 and 11. For any prime p strictly exceeding 11 only subgroups of index $p+1$, and no lower, are guaranteed to exist. Equivalently said, a modular equation, of prime level $p \geq 5$,

[1]The group G_p might be viewed as the Galois group (in the common sense) of its corresponding algebraic equations, as we shall further clarify. The standard notation for G_p is $\mathrm{PSL}(2,\mathbb{F}_p)$, where we assume the index p to denote a prime.

[2]The very concept of simplicity, being introduced by Galois, is the basis for classifying groups. The classification of finite simple groups, which referred to as "an enormous theorem", was (prematurely) announced in 1981 (by Daniel Gorenstein) before it was completed in 2004 (by Michael Aschbacher and Stephen Smith).

is depressable,[3] from degree $p+1$ to degree p, iff $p \in \{5,7,11\}$. Via explicitly constructing the subgroups, corresponding to these three exceptional primes, Galois must, in particular, be solely credited for actually solving the general quintic via exhibiting it as a modular equation of level 5. While Galois' contribution for formulating sufficient and necessary criterion for solubility of an algebraic equation via radicals is acknowledged, his decisive contribution to actually solving the quintic (before Hermite and Klein) is, surprisingly, too poorly recognized (if not at all unrecognized)! Betti, in 1851 [3], futily asked Liouville not to deprive the public any longer of Galois' (unpublished) results, and, in 1854 [4], went on to show that Galois' construction yields a solution to the quintic via elliptic functions.[4] One might associate with each quintic, given in Bring-Jerrard form, a corresponding value for the (Jacobi) elliptic modulus β, as Hermite did, in 1958 [6], implementing this very Galois' construction (thereby enabling an efficient algorithm for calculating the roots via values of an elliptic function at points placed apart by multiples of fifth-period). The group G_5 acts (naturally) on the projective line $\mathrm{P}\mathbb{Z}_5$, which six elements we shall, following Galois, label as 0,1,2,3,4 and ∞. Then collecting them in a triple-pair $\{(0,\infty),(1,4),(2,3)\}$, the group G_5 is seen to generate four more triple-pairs $\{(1,\infty),(2,0),(3,4)\}$,$\{(2,\infty),(3,1),(4,0)\}$,$\{(3,\infty),(4,2),(0,1)\}$,$\{(4,\infty),(0,3),(1,2)\}$. Together, the five triple-pairs constitute the five-element set upon which G_5 acts.[5] Galois did not (in his last letter) write down the four triple-pairs, which we did write after the first, and we now, guided by his conciseness and brevity, confine ourselves to writing down only the first pair-set that he presented for each of the two remaining cases, where $p=7$ and $p=11$, respectively: $\{(0,\infty),(1,3),(2,6),(4,5)\}$ and $\{(0,\infty),(1,2),(3,6),(4,8),(5,10),(9,7)\}$. Unlike the case $p=5$, an alternative might be presented for the case $p=7$, which is $\{(0,\infty),(1,5),(2,3),(4,6)\}$, and for the case $p=11$, which is $\{(0,\infty),(1,6),(3,7),(4,2),(5,8),(9,10)\}$. The "absolute invariant" for the action of the subgroup Γ_2, of the modular group $\Gamma := \mathrm{PSL}(2,\mathbb{Z})$, consisting of linear fractional transformations congruent to the identity modulo 2, is the square (of the elliptic

[3]This well-established term means lowerable. Its conception is a simple (yet ingenious) idea with which Galois alone must be fully credited, and, as we shall soon see, is the single most crucial (yet rarely brought to awareness) step towards actually solving the quintic.

[4]In 1830, Galois competed with Abel and Jacobi for the grand prize of the French Academy of Sciences. Abel (posthumously) and Jacobi were awarded (jointly) the prize, whereas all references to Galois' work (along with the work itself!) have (mysteriously) disappeared. The very fact that Galois' lost works contained contributions to Abelian integrals is either unknown (to many) or deemed (by some) no longer relevant to our contemporary knowledge. For the sake of being fair to a few exceptional mathematicians, we must cite (without translating to English) Grothendick (as a representative), who (in his autobiographical book Récoltes et Semailles) graciously admits that "Je suis persuadé d'ailleurs qu'un Galois serait allé bien plus loin encore que je n'ai été. D'une part à cause de ses dons tout à fait exceptionnels (que je n'ai pas reçus en partage, quant à moi)."

[5]Indeed, it is the five-element set (not merely a five-element set) which Hermite had no choice but to employ. Galois' construction for each of the two remaining cases, where $p=7$ or $p=11$, allows an alternative, as will, next, be exhibited.

modulus) β^2. A fundamental domain $\Gamma_2\backslash\mathcal{H}$, for the action of Γ_2 (on the upper half-plane $\mathcal{H}$), might be obtained by subjecting a fundamental domain $\Gamma\backslash\mathcal{H}$ (of Γ) to the action of the quotient group $\Gamma/\Gamma_2 \cong S_3$.[6] In particular, β^2 viewed as function on $\mathcal{H}$, is periodic, with period 2. Sohnke, in a remarkable work [7], had determined the modular equations for $\beta^{1/4}$, for all odd primes up to, and including, the prime 19. That work, along with Betti's work, inspired Hermite to (successfully) relate a (general) quintic, in Bring-Jerrard form, to a modular equation of level 5, yet he had little choice but to admit the importance of a sole Galois idea (in depressing the degree of the modular equation).[7] The modular polynomial for $\beta^{1/4}$, of level 5, is

$$\phi_5(x,y) := x^6 - y^6 + 5\,x^2y^2\,(x^2-y^2) + 4\,x\,y\,(1-x^4y^4),$$

and the period of $\beta^{1/4}$ (as an analytically continued function) is 16. Denoting the roots of $\phi_5(x,\, y=\beta^{1/4}(\tau))$, for a fixed $\tau\in\mathcal{H}$, by

$$y_5 = \beta^{1/4}(5\,\tau),\ y_m = -\beta^{1/4}\left(\frac{\tau+16\,m}{5}\right),\ 0\le m\le 4,$$

one calculates the minimal polynomial for $x_1 := (y_5-y_0)(y_4-y_1)(y_3-y_2)\,y$. It turns out to be

$$x^5 - 2000\,\beta^2\,(1-\beta^2)^2\,x + 1600\sqrt{5}\,\beta^2\,(1-\beta^2)^2\,(1+\beta^2).$$

Thereby, a root of the quintic

$$x^5 - x + c,\ c := \frac{2\,(1+\beta^2)}{5^{5/4}\sqrt{\beta(1-\beta^2)}} = \frac{2\,(1+y^8)}{5^{5/4}\,y^2\sqrt{1-y^8}},$$ [8]

is

$$\frac{\sqrt{5}\,c\,x_1}{4\,(1+\beta^2)} = \frac{x_1}{2\,\sqrt{5\sqrt{5}\,\beta(1-\beta^2)}} = \frac{(y_5-y_0)(y_4-y_1)(y_3-y_2)}{2\,y\,\sqrt{5\sqrt{5}\,(1-y^8)}},$$

---

[6] The latter quotient group coincides with G_2 which is isomorphic with S_3.

[7] Hermite had apparently adopted Cauchy's catholic and monarchist ideology, much in contrast to Galois' passionate rejection of social prejudice. In 1849, Hermite submitted a memoir to the French Academy of Sciences on doubly periodic functions, crediting Cauchy, but a priority dispute with Liouville prevented its publication. Hermite was then elected to the French Academy of Sciences on July 14, 1856, and (likely) acquainted, by Cauchy, with ideas stemming from (but not attributed to) Galois "lost" papers. T. Rothman made a pitiful attempt in "Genius and Biographers: The Fictionalization of Evariste Galois", which appeared in the American Mathematical Monthly, vol. 89, 1982, pp. 84-106 (and, sorrowly, received the Lester R. Ford Writing Award in 1983) to salvage Cauchy's reputation (unknowingly) suggesting further evidence of Cauchy's cowardice, and surprising us, along the way, with many (unusual but ill substantiated and biased) judgements telling us much about T. Rothman himself, but hardly anything trustworthy about anyone else!

[8] One must note that the constant coefficient c is invariant under the inversions $\beta\mapsto -1/\beta$ and $\beta\mapsto (1-\beta)/(1+\beta)$. Here, the composition of the latter two inversions is another inversion. The corresponding four-point orbit in a fundamental domain $\Gamma_2\backslash\mathcal{H}$ is generated via the mapping $\tau\mapsto 2/(2-\tau)$.

and so is expressible via the coefficients λ_m and μ_m of the elliptic polynomials $r_{m5}(x) = x^2 - \lambda_m x + \mu_m$, $0 \le m \le 5$.[9] In fact, the polynomials r_{m5} might be so ordered so that, for each m, the value β_m^2 coincides with y_m^8. The (general) expression for $y_m^8 = \beta_m^2$ might be written as

$$y_m^8 = \frac{s(\lambda_m,\, \mu_m,\, \beta)}{\beta^4 s(\lambda_m,\, \mu_m,\, 1/\beta)},$$

where

$$s(\lambda,\, \mu,\, x) = \left(\frac{1+\lambda\, x}{\mu} + x^2\right)\left(4\,\lambda + \left(\frac{2\,\lambda^2}{\mu} + 4 + 5\,\mu\right)x + \lambda\left(\frac{2}{\mu} + 3\right)x^2 + x^3\right),$$

and the coefficients $\lambda_m = \gamma_m + (2\cdot\gamma_m)$ and $\mu_m = \gamma_m(2\cdot\gamma_m)$ satisfy

$$\prod_{m=0}^{5}\left(x^2 - \lambda_m\, x + \mu_m\right) = x^{12} + \frac{62\,x^{10}}{5} - 21\,x^8 - 60\,x^6 - 25\,x^4 - 10\,x^2 + \frac{1}{5} +$$

$$+\,\alpha\,x^3\left(x^8 + 4\,x^6 - 18\,x^4 - \frac{92\,x^2}{5} - 7\right) + \alpha^2 x^4\left(\frac{x^6}{5} - 3\,x^2 - 2\right) - \frac{\alpha^3 x^5}{5} = r_5(x),$$

where $\alpha := 4(\beta + 1/\beta)$. The roots γ_m and $2\cdot\gamma_m$,[10] $0 \le m \le 5$, of the division polynomial r_5 might be highly efficiently calculated via the algorithm provided in [1]. Calculating a pair, say γ_0 and γ_5, suffices, of course, for calculating all twelve roots via applying the addition formula along with the doubling formula, as told in [2].

Nowadays, oblivion has entirely replaced marvelling at Galois key step, towards solving the quintic, in depressing the degree of the modular equation, of level 5, from 6 to 5,[11] and Galois is merely mentioned, along with Abel, for determining that the quintic is not solvable via radicals. We hope that this (crippled) view of Galois (deeply constructive) theory would finally come to an end.

References

[1] Adlaj S. *Iterative algorithm for computing an elliptic integral* // Issues on motion stability and stabilization (2011), 104-110 (in Russian).

[2] Adlaj S. *Multiplication and division on elliptic curves, torsion points and roots of modular equations*. Available at `http://www.ccas.ru/depart/mechanics/TUMUS/Adlaj/ECCD.pdf`.

[9] The elliptic polynomials were presented, in 2014, at the 7th PCA conference (http://pca.pdmi.ras.ru/2014/program) in a talk titled "Modular polynomial symmetries", and at the 17th workshop on Computer Algebra (http://compalg.jinr.ru/Dubna2014/abstracts.html) in a talk titled "Elliptic and coelliptic polynomials". Details are provided in [2].

[10] Consistently with the notation employed in [2], $2\cdot\gamma_m$ signifies that the doubling formula has been applied to γ_m.

[11] For example, S. Vlăduţ (wrongfully) attributes, in his book "Kronecker's Jugendtraum and Modular Functions" (published by Gordon and Breach in 1991), to Hermite showing the equivalence of the general quintic to the modular equation of level 5.

[3] Betti E. *Sopra la risolubilità per radicali delle equazioni algebriche irriduttibili di grado primo* // Dagli Annali di Scienze matimatiche e fisiche, t. II (Roma, 1851): 5-19.

[4] Betti E. *Un teorema sulla risoluzione analitica delle equazioni algebriche* // Dagli Annali di Scienze matimatiche e fisiche, t. V (Roma, 1854): 10-17.

[5] Galois É. *"Lettre de Galois à M. Auguste Chevalier"* // Journal de Mathématiques Pures et Appliquées XI (1846): 408–415.

[6] Hermite C. *"Sur la résolution de l'équation du cinquième degré"* // Comptes Rendus de l'Académie des Sciences XLVI(I) (1858): 508–515.

[7] Sohnke L. *Equationes Modulares pro transformatione functionum Ellipticarum* // Journal de M. Crelle, t. XVI (1836): 97-130.

Semjon Adlaj
Section of Stability Theory and Mechanics of Controlled Systems
Department of Mechanics
Division of Complex Physical and Technical Systems Modeling
Computing Center of the Federal Research Center "Informatics and Control"
Russian Academy of Sciences
Russia 119333, Moscow, Vavilov Street 40.
e-mail: SemjonAdlaj@gmail.com

On the Extension of Adams–Bashforth–Moulton Methods for Numerical Integration of Delay Differential Equations and Application to the Moon's Orbit

Dan Aksim and Dmitry Pavlov

Abstract. One of the problems arising in modern celestial mechanics is the need of precise numerical calculation of the Moon's orbit. Due to the nature of tidal forces, their action is modeled with a time delay and the orbit is therefore described by a so-called delay differential equation (DDE). Numerical integration of the orbit is normally being performed in both directions (forwards and backwards in time) from some epoch, and while the theory of normal forward-in-time numerical integration of DDEs is developed and well-known, integrating a DDE backwards in time is equivalent to solving a special kind of DDE called an advanced-delay differential equation, where the derivative of the function depends on not yet known future states of the function, which presents a certain numerical challenge.

The present work examines a modification of Adams–Bashforth–Moulton method allowing to perform integration of the Moon's DDE forwards and backwards in time and the results of such integration.

Dan Aksim
Laboratory of Ephemeris Astronomy
Institute of Applied Astronomy of the Russian Academy of Sciences
St. Petersburg, Russia
e-mail: danaksim@iaaras.ru

Dmitry Pavlov
Laboratory of Ephemeris Astronomy
Institute of Applied Astronomy of the Russian Academy of Sciences
St. Petersburg, Russia
e-mail: dpavlov@iaaras.ru

Links between second-order Fuchsian equations and first-order linear Fuchsian systems

Mikhail Babich and Sergey Slavyanov

The simplest second-order Fuchsian equation is the hypergeometric equation with three Fuchsian singularities. The next in complexity is the Heun equation with four Fuchsian singularities. In addition to Fuchsian singularities apparent singularities can be added to both discussed equations and we arrive to deformed equations.

On the other hand, linear first-order systems with three or four Fuchsian singularities are studied. Clearly, each component of its solution satisfies second-order equation. The number of apparent singularities differs from zero to two according to degree of off-diagonal matrix element in the system.

The number of oarameters in the system is larger than that in the equation. Hence in order to find a needed relation between the given system and the equation it is needed to simplify the matrices – residues at finite Fuchsian singularities. The most simple way to do it is to choose either determinants or traces of these residues to be zero. Calculations for both cases are presented in the talk. Comparitions of these two approaches gives the possibility to find the relation between use of antiquantization procedure [1, 2] and isomonodromic property [3, 4] for derivation Painlevé equation P^{VI}.

References

[1] Slavyanov S. 2015 Antiquantization and the corresponding symmetries *Theoret. and Math. Phys.* **185** 1522-1526

[2] Slavyanov S 2017 Symmetries and apparent singularities for simplest fuchsian equations *Theoret. and Math. Phys.* **193** 1754-1760.

[3] Bolibruch A 2009 *Inverse problems of monodromie in analytical thery of differential equations* in russian, (Moscow - MNCMO)

[4] Its A and Novokshenov V 1986 *The isomonodromic deformation method in the theory of Painlevé equations* Lecture Notes in Math. **1191** (Springer - Berlin, New York)

Mikhail Babich
PDMI RAS RU
St.Petersburg, Russia
e-mail: mbabich@pdmi.ras.ru

Sergey Slavyanov
Saint-Petersburg State University,
St.Petersburg, Russia
e-mail: slav@ss2034.spb.edu

q-Analogue of discriminant set and its computation

Alexander Batkhin

Abstract. A generalization of the classical discriminant of the polynomial with arbitrary coefficients defined using the linear Hahn operator that decreases the degree of the polynomial by one is studied. The structure of the generalized discriminant set of the real polynomial, i.e., the set of values of the polynomial coefficients at which the polynomial and its Hahn operator image have a common root, is investigated. The structure of the generalized discriminant of the polynomial of degree n is described in terms of the partitions of n. Algorithms for the construction of a polynomial parameterization of the generalized discriminant set in the space of the polynomial coefficients are proposed. The main steps of these algorithms are implemented in a Maple library.

Introduction

Let $g : \mathbb{R} \to \mathbb{R} : x \mapsto g(x)$ be a given smooth one-to-one map of the real axis, which is the domain of polynomial $f(x)$ with arbitrary coefficients. We want to find conditions on the coefficients of the polynomial under which it has at least a pair of roots t_i, t_j satisfying the relation $g(t_i) = t_j$ and investigate the structure of the algebraic variety in the space of coefficients possessing such property.

Here we consider a generalization of the classical discriminant of the polynomial. This generalization naturally includes the classical discriminant and its analogs emerging when the q-differential and difference operators that have a well-developed calculus [1] and important applications [2] are used. It turned out that the constructs that were earlier obtained for investigating the discriminant [3] and resonance sets [4] can be extended for a more general case.

The aim of this research is to propose an efficient algorithm for calculating the parametric representation of all components of the g-discriminant set $\mathcal{D}_g(f)$ of the monic polynomial $f(x)$.

1. Generalized discriminant set

Definition 1. Define the q**-bracket** $[a]_q$, q**-Pochhammer symbol** $(a;q)_n$, q**-factorial** $[n]_q!$, q**-binomial coefficients (Gaussian) coefficients** $\begin{bmatrix} n \\ k \end{bmatrix}_q$ as follows:

$$[a]_q = \frac{q^a - 1}{q - 1}, a \in \mathbb{R}\backslash\{0\}, \quad (a;q)_n = \prod_{k=0}^{n-1} \left(1 - aq^k\right), (a;q)_0 = 1,$$

$$[n]_q! = \prod_{k=1}^{n} [k]_q = \frac{(q;q)_n}{(1-q)^n}, q \neq 1, \quad \begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{[n]_q!}{[n-k]_q!\,[k]_q!} = \prod_{i=1}^{k} \frac{q^{n-i+1} - 1}{q^i - 1}.$$

As $q \to 1$, all these objects become classical.

Define a g-analogue of the standard binomial $(x-a)^n$ so called g-binomial

$$\{x;t\}_{n;g} \equiv \prod_{i=0}^{n-1} (x - g^i(t)), \quad \{x;t\}_{0;q} = 1.$$

Here g^k is the k-th iteration of the diffeomorphism g, $k \in \mathbb{Z}$ (see below).

Let $f_n(x)$ be is a monic polynomial of degree n with complex coefficients defined by

$$f_n(x) \stackrel{\text{def}}{=} x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n.$$

Let $\mathbb{P}$ be the space of polynomials over $\mathbb{R}$ and let g

$$g : \mathbb{R} \to \mathbb{R} : x \mapsto qx + \omega, \quad q, \omega \in \mathbb{R}, \quad q \neq \{-1, 0\},$$

be a linear diffeomorphism on $\mathbb{R}$ that induces a linear **Hahn operator** $\mathcal{A}_{\mathrm{g}}$ on $\mathbb{P}$, satisfying the following two conditions:

1. the degree reduction: $\deg(\mathcal{A}_{\mathrm{g}}\, f_n)(x) = n - 1$; in particular, $\mathcal{A}_{\mathrm{g}}\, x = 1$;
2. Leibnitz rule analogue:

$$(\mathcal{A}_{\mathrm{g}}\, x f_n)(x) = f_n(x) + g(x)(\mathcal{A}_{\mathrm{g}}\, f_n)(x).$$

The Hahn operator $\mathcal{A}_{\mathrm{g}}$ called below g**-derivative** has the form

$$(\mathcal{A}_{\mathrm{g}}\, f)(x) \stackrel{\text{def}}{=} \begin{cases} \dfrac{f(qx+\omega) - f(x)}{(q-1)x + \omega}, & x \neq \omega_0, \\ f'(\omega_0), & x = \omega_0, \end{cases} \tag{1}$$

where $\omega_0 = \omega/(1-q)$ is the fixed point of g. Parameters q and ω are satisfied the following conditions $q, \omega \in \mathbb{R}$, $q \neq \{-1, 0\}$ and $(q, \omega) \neq (1, 0)$. The g-derivative $\mathcal{A}_{\mathrm{g}}$ can be considered as a generalization of the q-differential Jackson operator $\mathcal{A}_q$ at $\omega = 0$, $q \neq 1$, as the difference operator Δ_ω at $q = 1$ and as the classical derivative d/dx in the limit $q \to 1$ and $\omega = 0$.

q-Analogs of many mathematical objects emerged already in Euler's works, and then were elaborated by many mathematicians (see the historical review in [1]). The q-calculus has recently became a part of the more general construct called quantum calculus [5]. It has numerous applications in various fields of modern mathematics and theoretical physics. For example, many applications related to

the theory of orthogonal polynomials and their various generalizations, it is important to determine the conditions on the coefficients a_i, $i = 1, \ldots, n$, of the polynomial $f_n(x)$ under which it has roots satisfying $g(t_i) = t_j$.

Definition 2. The pair of roots t_i, t_j, $i, j = 1, \ldots, n$, $i \neq j$ of the polynomial $f_n(x)$ is said to be g**-coupled** if $g(t_i) = t_j$.

Let consider the following problem.

Problem. In the coefficient space $\Pi \equiv \mathbb{C}^n$ of the polynomial $f_n(x)$, investigate the g**-discriminant set** denoted $\mathcal{D}_g(f_n)$ on which this polynomial has at least one pair of g-coupled roots.

Definition 3. The sequence $\mathrm{Seq}_g^{(k)}(t_1)$ of g-coupled roots of length k is defined as the finite sequence $\{t_i\}$, $i = 1, \ldots, k$ in which each term, beginning with the second one, is a g-coupled root of the preceding term: $g(t_i) = t_{i+1}$. The initial root t_1 is called the generating root of the sequence $\mathrm{Seq}_g^{(k)}(t_1)$.

For each fixed set of parameters q, ω, the g-discriminant set $\mathcal{D}_g(f_n)$ consists of a finite set of varieties $\mathcal{V}_k$ on each of which $f_n(x)$ has k sequences $\mathrm{Seq}_g^{(l_i)}(t_i)$ of g-coupled roots of length $_i$ with different generating roots t_i, $i = 1, \ldots, k$. To obtain an expression for the generalized (sub)discriminant of the polynomial $f_n(x)$ in terms of its coefficients, any method available in the classical elimination theory can be used. If we replace the derivative $f_n'(x)$ by the polynomial $\mathcal{A}_g f_n(x)$, then any matrix method for calculating the resultant of a pair of polynomials gives an expression of the generalized k-th subdiscriminant $D_g^{(k)}(f_n)$ (see [6, 3] for details).

Theorem 1. *The polynomial $f_n(x)$ has exactly $n-d$ different sequences of g-coupled roots, iff the first nonzero element in the sequence of i-th generalized subdiscriminants $D_g^{(i)}(f_n)$ is the subdiscriminat $D_g^{(d)}(f_n)$ with the index d.*

2. Algorithm of parametrization of $\mathcal{D}_g(f_n)$ and its implementation

Definition 4. The partition λ of a natural number n is any finite nondecreasing sequence of natural numbers $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_k$, for which $\sum_{i=1}^{k} \lambda_i = n$. Each partition λ will be written as $\lambda = [1^{n_1} 2^{n_2} 3^{n_3} \ldots]$.

Consider the partition $\lambda = [1^{n_1} 2^{n_2} 3^{n_3} \ldots]$ of the natural number n. The quantity i in the partition λ determines the length of the sequence of g-coupled roots for the corresponding generating root t_i, and n_i is the number of different generating roots determining the sequence of roots of length i. Every partition λ of n determines the structure of the g-coupled roots of the polynomial $f_n(x)$, and this structure is associated with the algebraic variety $\mathcal{V}_l^i$, $i = 1, \ldots, p_l(n)$ of dimension l corresponding to the number of different generating roots t_i in the coefficient space Π.

Consider the partition $\left[n^1\right]$ corresponding to the case when there is a unique sequence of roots of length n specified by the generating root t_1. Then, the polynomial $f_n(x)$ is a g-binomial $\{x;t_1\}_{n;g}$ and its coefficients a_i can be represented in terms of the elementary symmetric polynomials $\sigma_i(x_1,x_2,\ldots,x_n)$ calculated on the roots $g^j(t_1)$, $j=0,\ldots,n-1$,

$$a_i=(-1)^i\sigma_i\left(t_1,g(t_1),\ldots,g^{n-1}(t_1)\right),\ i=1,\ldots,n.$$

Let consider the polynomial $f_n(x)\equiv\{x;t_1\}_{n;g}$ with the structure of roots corresponding to the partition $\left[n^1\right]$. Using [7, Lemmas 2, 3], we conclude that, for every k such that $0<k\le n$, it holds that

$$\sum_{i=0}^{k}\begin{bmatrix}n\\i\end{bmatrix}_q\frac{[n-i]_q!}{[n]_q!}\left(\mathcal{A}_{\mathrm{g}}{}^i\,f_n\right)(t_1)\{t_2;t_1\}_{i;g}=f_k(x;t_2)\cdot f_{n-k}(x;g^k(t_1)),\qquad(2)$$

where $(\mathcal{A}_{\mathrm{g}}{}^0\,f)(x)\equiv f(x)$. Therefore, formula (2) allows us to pass from the polynomial with the structure of roots corresponding to the partition $\left[n^1\right]$ to a polynomial with the structure of roots determined by the partitions $\left[k^1(n-k)^1\right]$ or $\left[(n/2)^2\right]$, if $k=n/2$.

Theorem 2. *Let there be a variety $\mathcal{V}_l$, $\dim\mathcal{V}_l=l$ on which the polynomial $f_n(x)$ has different sequences of g-coupled roots and the sequence of roots $\mathrm{Seq}_g^{(m)}(t_1)$ has length $m>1$. The roots of the other sequences are not g-coupled with all roots of the sequence $\mathrm{Seq}_g^{(m)}(t_1)$. Let $\mathbf{r}_l(t_1,\ldots,t_l)$ be a parameterization of the variety $\mathcal{V}_l$. Then for $0<k<n$, the formula*

$$\mathbf{r}_l(t_1,\ldots,t_l,t_{l+1})=\mathbf{r}_l(t_1,\ldots,t_l)+\sum_{i=1}^{k}\begin{bmatrix}k\\i\end{bmatrix}_q\frac{[m-i]_q!}{[m]_q!}\left(\mathcal{A}_{\mathrm{g}}{}^i\,\mathbf{r}_l\right)(t_1)\{t_{l+1};t_1\}_{i;g}$$

specify a parameterization of the part of $\mathcal{V}_{l+1}$ on which there are two sequences of roots $\mathrm{Seq}_g^{(m-k)}(g^k(t_1))$ and $\mathrm{Seq}_g^{(k)}(g(t_{l+1}))$, and the other sequences of roots are the same as on the original variety $\mathcal{V}_l$.

We introduce two basic operations that allow us to successively pass from the parametric representation of the one-dimensional variety $\mathcal{V}_1$ to the parameterization of all other components of the g-discriminant set $\mathcal{D}_g(f_n)$.

1. The operation of passing from the variety $\mathcal{V}_l$ to the variety $\mathcal{V}_{l+1}$ in Theorem 2 is called **ASCENT** of order k. If $f_n(x)$ has only real roots on this variety, then we obtain its complete parameterization; if there are complex roots, then we apply the following operation.
2. The operation called **CONTINUATION** makes it possible to obtain a parameterization of the entire variety $\mathcal{V}_{l+1}$ obtained by the **ASCENT** operation in the case when there are complex conjugate roots on it.

At each step of this algorithm, we remain within polynomial parameterizations; therefore, the following result holds.

Proposition. For fixed values of parameters (q, ω) of the Hahn operator (1), the g-discriminant set $\mathcal{D}_g(f_n)$ of the polynomial $f_n(x)$ admits a polynomial parameterization of each of the algebraic varieties $\mathcal{V}_l^k$, $l = 1, \ldots, n-1$, $k = 1, \ldots, p_l(n)$, that form this set.

For calculating the g-discriminant set $\mathcal{D}_g(f_n)$, a number of procedures in `Maple` and `Sympy` were developed. Their description and application to some examples are given in [8].

References

[1] T. Ernst. *A Comprehensive Treatment of q-Calculus*. Springer, Basel Heidelberg New York Dordrecht London, 2012. http://dx.doi.org/10.1007/978-3-0348-0431-8 doi:10.1007/978-3-0348-0431-8.

[2] R. Koekoek, P. A. Lesky, and R. F. Swarttouw. *Hypergeometric Orthogonal Polynomials and Their q-Analogues*. Springer-Verlag, Berlin Heidelberg, 2010. http://dx.doi.org/10.1007/978-3-642-05014-5 doi:10.1007/978-3-642-05014-5.

[3] A. B. Batkhin. Parameterization of the discriminant set of a polynomial. *Programming and Computer Software*, 42(2):65–76, 2016. http://dx.doi.org/10.1134/S0361768816020031 doi:10.1134/S0361768816020031.

[4] A. B. Batkhin. Structure of the resonance set of a real polynomial. *Keldysh Institute Preprints*, (29), 2016. (in Russian). URL: http://www.keldysh.ru/papers/2016/prep2016_29.pdf, http://dx.doi.org/10.20948/prepr-2016-29 doi:10.20948/prepr-2016-29.

[5] V. Kac and P. Cheung. *Quantum Calculus*. Springer-Verlag, New York, Heidelber, Berlin, 2002.

[6] Gathen, J. von zur and T. Lücking. Subresultants revisited. *Theoretical Computer Science*, 297:199–239, 2003. http://dx.doi.org/10.1016/S0304-3975(02)00639-4 doi:10.1016/S0304-3975(02)00639-4.

[7] A. B. Batkhin. Parameterization of a set determined by the generalized discriminant of a polynomial. *Programming and Computer Software*, 44(2):75–85, 2018. http://dx.doi.org/10.1134/S0361768818020032 doi:10.1134/S0361768818020032.

[8] A. B. Batkhin. Computation of generalized discriminant of a real polynomial. *Keldysh Institute Preprints*, (88), 2017. (in Russian). URL: http://www.keldysh.ru/papers/2017/prep2017_88.pdf, http://dx.doi.org/10.20948/prepr-2017-88 doi:10.20948/prepr-2017-88.

Alexander Batkhin
Department of Singular Problems
Keldysh Institute of Applied Mathematics of RAS
Department of Theoretical Mechanics
Moscow Institute of Physics and Technology
Moscow, Russia
e-mail: batkhin@gmail.com

Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game.

Michela Ceria and Teo Mora

Abstract. In 1990 Cerlienco and Mureddu gave a combinatorial iterative algorithm which, given an ordered set of points, returns the lexicographical Gröbner escalier of the ideal of these points. There are many alternatives to this algorithm; the most efficient is the Lex Game, which is not iterative on the points, but its performances are definitely better.
In this paper, we develop an iterative alternative to Lex Game algorithm, whose performances are very near to those of the original Lex Game, by means of the Bar Code, a diagram which allows to keep track of information on the points and the corresponding monomials, that are lost and usually recomputed many times in Cerlienco-Mureddu algorithm. Using the same Bar Code, we will also give an efficient algorithm to compute squarefree separator polynomials of the points and the Auzinger-Stetter matrices with respect to the lexicographical Gröbner escalier of the ideal of the points.

Extended abstract

In 1990 Cerlienco and Mureddu [5, 6, 7] gave a combinatorial algorithm which, given an ordered set of points $\underline{\mathbf{X}} = [P_1, ..., P_N] \subset \mathbf{k}^n$, $\mathbf{k}$ a field, returns the lexicographical Gröbner escalier

$$\underline{\mathsf{N}(I(\mathbf{X}))} \subset \mathcal{T} := \{x^\gamma := x_1^{\gamma_1} \cdots x_n^{\gamma_n} \,|\, \gamma := (\gamma_1, ..., \gamma_n) \in \mathbb{N}^n\}$$

of the vanishing ideal

$$I(\mathbf{X}) := \{f \in \mathcal{P} : \, f(P_i) = 0, \, \forall i \in \{1, ..., N\}\} \subset \mathcal{P} := \mathbf{k}[x_1, ..., x_n].$$

Such algorithm actually returns a bijection (labelled *Cerlienco-Mureddu correspondence* in [12, II,33.2])

$$\Phi_{\underline{\mathbf{X}}} : \underline{\mathbf{X}} \to \underline{\mathsf{N}(I(\mathbf{X}))}.$$

The algorithm is inductive and thus has complexity $\mathcal{O}\left(n^2 N^2\right)$, but it has the advantage of being iterative, in the sense that, given an ordered set of points

$\underline{\mathbf{X}} = [P_1, ..., P_N]$, its related escalier $\overline{\mathsf{N}(I(\mathbf{X}))}$ and correspondence $\Phi_{\underline{\mathbf{X}}}$, for any point $Q \notin \underline{\mathbf{X}}$ it returns a term $\tau \in \mathcal{T}$ such that, denoting $\underline{\mathbf{Y}}$ the ordered set $\underline{\mathbf{Y}} := [P_1, ..., P_N, Q]$,

- $\overline{\mathsf{N}(I(\mathbf{Y}))} = \overline{\mathsf{N}(I(\mathbf{X}))} \sqcup \{\tau\}$,
- $\overline{\Phi_{\underline{\mathbf{Y}}}(P_i)} = \overline{\Phi_{\underline{\mathbf{X}}}(P_i)}$ for all i and $\tau = \Phi_{\underline{\mathbf{Y}}}(Q)$.

In order to produce the lexicographical Gröbner escalier with a better complexity, [8] gave a completely different approach (*Lex Game*): given a set of (not necessarily ordered) points $\mathbf{X} = \{P_1, ..., P_N\} \subset \mathbf{k}^n$ they built a trie (*point trie*) representing the coordinates of the points and then used it to build a different trie, the *lex trie*, which allows to reed the lexicographical Gröbner escalier $\mathsf{N}(I(\mathbf{X}))$. Such algorithm has a very better complexity, $\mathcal{O}(nN + N\min(N, nr))$, where $r < n$ is the maximal number of edges from a vertex in the point tree, but in order to obtain it, [8] was forced to give up iterativity.

In 1982 Buchberger and Möller [2] gave an algorithm (*Buchberger-Möller algorithm*) which, for any term-ordering $<$ on $\mathcal{T}$ and any set of (not necessarily ordered) points $\mathbf{X} = \{P_1, ..., P_N\} \subset \mathbf{k}^n$ iterating on the $<$-ordered set $\mathsf{N}(I(\mathbf{X}))$, returns the Gröbner basis of $I(\mathbf{X})$ with respect $<$, the set $\mathsf{N}(I(\mathbf{X}))$ and a family $[f_1, \cdots, f_N] \subset \mathcal{P}$ of separators of $\mathbf{X}$ *id est* a set of polynomials s.t. $f_i(P_j) = \delta_{ij}$.
Later Möller [11] extended the same algorithm to any finite set of functionals defining a 0-dimensional ideal, thus absorbing also the FGLM-algorithm and, on the other side, proving that Buchberger-Möller algorithm has the FGLM-complexity $\mathcal{O}(n^2N^3f)$ where f is the avarage cost of evaluating a functional at a term[1].
Möller [11] gave also an alternative algorithm (*Möller algorithm*) which, for any term-ordering $<$ on $\mathcal{T}$, given an ordered set of points[2] $[P_1, ..., P_N] \subset \mathbf{k}^n$, for each $\sigma \leq N$, denoting $\mathbf{X}_\sigma = \{P_1, ..., P_\sigma\}$ returns, with complexity $\mathcal{O}(nN^3 + fnN^2)$

- the Gröbner basis of the ideal $I(\mathbf{X}_\sigma)$;
- the correlated escalier $\mathsf{N}(I(\mathbf{X}_\sigma))$;
- a term $t_\sigma \in \mathcal{T}$ such that $\mathsf{N}(I(\mathbf{X}_\sigma) = \mathsf{N}(I(\mathbf{X}_{\sigma-1})) \sqcup \{\tau\}$,
- a triangular set $\{q_1, \cdots, q_\sigma\} \subset \mathcal{P}$ s.t. $q_i(P_j) = \delta_{i,j}$
- whence a family of separators can be easily deduced by Gaussian reduction,
- a bijection Φ_σ such that $\Phi_\sigma(P_i) = \tau_i$ for each $i \leq \sigma$, which moreover if $<$ is lexicographical, then coincides with Cerlienco-Mureddu corresondence.

Later, Mora [12, II,29.4] remarked that, since the complexity analisis of both Buchberger-Möller and Möller algorithm were assuming to perform Gaussian reduction on an N-square matrix and to evaluate each monomial in the set

$$\mathsf{B}(I(\mathbf{X})) := \{\tau x_j, \tau \in \mathsf{N}(I(\mathbf{X}_\sigma)), 1 \leq j \leq n\}$$

[1] A more precise evaluation was later given by Lundqvist[9], namely

$$\mathcal{O}(\min(n, N)N^3 + nN^2 + nNf + \min(n, N)N^2f).$$

[2] Actually the algorithm is stated for an ordered finite set of functionals $[\ell_1, ..., \ell_N] \subset \mathrm{Hom}_{\mathbf{k}}(\mathcal{P}, \mathbf{k})$ such that for each $\sigma \leq N$ the set $\{f \in \mathcal{P} : \ell_i(f) = 0, \forall i \leq s\}$ is an ideal.

over each point $P_i \in \mathbf{X}$, within that complexity one can use all the information which can be deduced by the computations $\tau(P_i), \tau \in \mathsf{B}(I(\mathbf{X})), 1 \leq i \leq N$; he therefore introduced the notion of *structural description* of a 0-dimensional ideal [12, II.29.4.1] and gave an algorithm which computes such structural description of each ideal $I(\mathbf{X}_\sigma)$. Also anticipating the recent mood of degrobnerizing effective ideal theory, Mora, in connection with Auzinger-Stetter matrices and algorithm [1] proposed to present a 0-dimensional ideal $I \subset \mathcal{P}$ and its quotient algebra $\mathcal{P}/I$ by giving its *Gröbner representation* [12, II.29.3.3] *id est* the assignment of

- a $\mathbf{k}$-linearly independent ordered set $[q_1, \ldots, q_N] \subset \mathcal{P}/I$
- n N-square matrices $\left(a_{lj}^{(h)}\right), 1 \leq h \leq n$,

which satisfiy

1. $\mathcal{P}/I \cong \mathrm{Span}_{\mathbf{k}}\{q_1, \ldots, q_N\}$,
2. $x_h q_l = \sum_j a_{lj}^{(h)} q_j, 1 \leq j, l \leq N, 1 \leq h \leq n$.

Since Möller algorithm and Mora's extension is inductive, our aim is to give an algorithm which given an ordered set of points $\mathbf{X} = [P_1, ..., P_N] \subset \mathbf{k}^n$ produces for each $\sigma \leq N$

- the lexicographical Gröbner escalier $\mathsf{N}(I(\mathbf{X}_\sigma))$, the related Cerlienco-Mureddu corresondence,
- a family of squarefree separators for $\mathbf{X}_\sigma$,
- the n N-square Auzinger-Stetter matrices $\left(a_{lj}^{(h)}\right), 1 \leq h \leq n$, which satisfy condition 2. above with respect the linear basis $\mathsf{N}(I(\mathbf{X}_\sigma))$.

The advantage is that, any time a *new* point is to be considered, the old data do not need to be modified and actually can simplify the computation of the data for the new ideal.

Since the Lex Game approach which has no tool for considering the order of the points has no way of using the data computed for the ideal $I(\mathbf{X}_{\sigma-1})$ in order to deduce those for $I(\mathbf{X}_\sigma)$, while Möller algorithm and Mora's extension are iterative on the ordered points and intrinsecally produce Cerlienco-Mureddu correspondence, in order to achieve our aim, we need to obtain a variation of Cerlienco-Mureddu algorithm which is not inductive.

Our tool is the Bar Code [3, 4], essentially a reformulation of the point trie which describes in a compact way the combinatorial strucure of a (non necessarily 0-dimensional) ideal; the Bar Code allows to remember and reed those data which Cerlienco-Mureddu algorithm is forced to inductively recompute. Actually, once the point trie is computed as in [8] with inductive complexity $\mathcal{O}(N \cdot N \log(N) n)$. the application of the Bar Code allows to compute the lexicographical Gröbner escaliers $\mathsf{N}(I(\mathbf{X}_\sigma))$ and the related Cerlienco-Mureddu correspondences, with iterative complexity

$$\mathcal{O}(N \cdot (n + \min(N, nr) \sim \mathcal{O}(N \cdot nr).$$

The families of separators can be iteratively obtain using Lagrange interpolation via data easily deduced from the point trie as suggested in [8, 9] with complexity $\mathcal{O}(N \cdot \min(N, nr)$.

The computation of the Auzinger-Stetter matrices is based on Lundqvist result [10, Lemma 3.2] and can be inductively performed with complexity[3] $\mathcal{O}\left(N \cdot (nN^2)\right)$.

References

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

[2] Möller H.M., Buchberger B., *The construction of multivariate polynomials with preassigned zeros*, L. N. Comp. Sci. 144 (1982), 24–31, Springer

[3] Ceria, M., *Bar Code for monomial ideals*, submitted to Journal of Symbolic Computations, special issue for MEGA 2017.

[4] Ceria, M., *Applications of Bar Code to involutive divisions and a greedy algorithm for complete sets.*, submitted

[5] Cerlienco L., Mureddu M., *Algoritmi combinatori per l'interpolazione polinomiale in dimensione* ≥ 2, preprint (1990).

[6] Cerlienco L., Mureddu M., *From algebraic sets to monomial linear bases by means of combinatorial algorithms*, Discrete Math. 139, $73 - 87$.

[7] Cerlienco L., Mureddu M., *Multivariate Interpolation and Standard Bases for Macaulay Modules*, J. Algebra 251 (2002), $686 - 726$.

[8] Felszeghy B., Ráth B., Rónyai L., *The lex game and some applications*, J. Symbolic Computation 41 (2006), $663 - 681$.

[9] Lundqvist S., *Complexity of comparing monomials and two improvements of the BM-algorithm.* L. N. Comp. Sci. 5393 (2008), 105–125, Springer

[10] Lundqvist S., *Vector space bases associated to vanishing ideals of points*, Journal of Pure and Applied Algebra, 214, Issue 4, (2010), pagg $309 - 321$.

[11] Marinari M.G, Mora T., Moeller H.M., *Gröbner bases of ideals defined by functionals with an application to ideals of projective points* , Appl. Algebra Engrg. Comm. Comput. 4 (1993), 103-145.

[12] Mora T., *Solving Polynomial Equation Systems* 4 Vols., Cambridge University Press, I (2003), II (2005), III (2015), IV (2016).

Michela Ceria
Department of Computer Science University of Milan Milano, Italy
e-mail: michela.ceria@gmail.com

Teo Mora
Department of Mathematics University of Genoa Genoa, Italy
e-mail: theomora@disi.unige.it

[3] Naturally, our decision of giving an algorithm which can produce data for the the vanishing ideal when a new point is considered forbid us of using the new better algorithms for matrix multiplication; thus our complexity is $\mathcal{O}\left(N^3\right)$ and not $\mathcal{O}\left(N^\omega\right), \omega < 2.39$.

Bifurcation diagrams for polynomial nonlinear ordinary differential equations

Daria Chemkaeva and Alexandr Flegontov

Abstract. This study considers the general case for classes of nonlinear boundary value problems for a second-order autonomous ordinary differential equation with homogeneous boundary conditions. The general case is studied applying to polynomial-like nonlinearities. We investigate the number of positive solutions to the problem. The research is confirmed by computer-generated function of P. Korman, Y. Li, T. Ouyang Theorem and bifurcation diagrams.

Introduction

We study the existence of positive solutions of the nonlinear two-point boundary value problem:

$$y''_{xx} + \lambda f(y(x)) = 0, \quad x \in (-1; 1), \tag{1}$$

$$y(-1) = y(1) = 0. \tag{2}$$

Assume $f = f(y)$ so second order ODE is autonomous, where parameter λ is positive. In this case, the bifurcation arises when the number of solutions of the differential equation changes as the parameter λ changes.

The problem (1)–(2) describes many physical processes, for example, belongs to the problems of combustion of gases and population dynamics. The nonlinearity of $f = f(y)$ in combustion theory denotes intermediate steady states of the temperature distribution y, and the bifurcation parameter λ determines the amount of unburnt substance.

Section 1 is technical and contains useful supplement of P. Korman, Y. Li and T. Ouyang theorem. Section 2 is the main part of the study where the behavior of function from P. Korman, Y. Li and T. Ouyang Theorem is studied considering that nonlinear function is a polynomial of odd degree with a_{2n-1} roots ($n = 2, \ldots, k, k \geq 2$). The examples are provided with description of the respective time-map functions, solutions, bifurcations and visualizations. Finally, we summarize the results and make conclusions.

1. P. Korman, Y. Li and T. Ouyang Theorem

The differential equation (1) with boundary conditions (2) has k zeros of solutions depending on the bifurcation parameter. Let us consider the case when the number of zeros of the solutions is even. In this case, solutions (1)–(2) are symmetric with respect to $x = 0$ [1], hence (1)–(2) can be reduced to the form:

$$y''_{xx} + \lambda f(y(x)) = 0, \quad x \in (0; 1), \tag{3}$$

$$y'_x(0) = 0, \quad y(1) = 0. \tag{4}$$

It is known that positive solutions can be determined using term $y(0) = a$. This zero function is a time-map for solutions (1)–(2) [2] and the maximal value of the solution of the boundary value problem, which uniquely determines the pair $(\lambda, y(x))$. We show that by defining a we can uniquely determine the appropriate value $\lambda > 0$ and the solution of the problem $y = y(x)$.

Suppose that $t = \sqrt{\lambda}x$ so for the function $y = y(t)$ we consider the intermediate Cauchy problem:

$$y''_{tt} + f(y) = 0, \tag{5}$$

$$y'_t(0) = 0, \quad y(0) = a. \tag{6}$$

We use the substitution and find the first integral of equation (5), fulfilling the first boundary condition (6):

$$y'_t = \sqrt{2}\sqrt{F(a) - F(y)}, \quad F(y) = \int\limits_0^y f(y)\, dy.$$

For the existence of the solution (5)–(6) it is necessary to satisfy the inequality $F(a) \geq F(y)$. The solution of boundary value problem (5)–(6) in implicit form is:

$$t = \int\limits_0^y \frac{dt}{\sqrt{F(a) - F(t)}}.$$

Returning to boundary value problem (3)–(4), the bifurcation parameter is:

$$\lambda(a) = \frac{1}{2}\Big[\int\limits_0^a \frac{dt}{\sqrt{F(a) - F(t)}}\Big]^2. \tag{7}$$

The function $\lambda = \lambda(a)$ is called the bifurcation curve; its turning points are bifurcation points. The plot of this function is called the bifurcation diagram [3], implying an image of the change in the possible dynamic modes of the system with a change in the value of bifurcation parameter λ.

The authors P. Korman, Y. Li and T. Ouyang prove that a solution of the problem (1)–(2) with the maximal value $a = y(0)$ is singular if and only if

$$G(a) \equiv \sqrt{F(a)} \int\limits_0^a \frac{f(a) - f(\tau)}{[F(a) - F(\tau)]^{3/2}}\, d\tau - 2 = 0, \tag{8}$$

where $F(y) = \int_0^y f(t)\,dt$.

2. Nonlinearity as a polynomial of odd degree

Now we study the general case, assuming that the function $f(y)$ is a polynomial, and consequently can change the sign.

We set

$$f(y) = (y - a_1)(y - a_2)(y - a_3)...(y - a_{2n-2})(a_{2n-1} - y), \tag{9}$$

where $0 < a_1 < a_2 < ... < a_{2n-2} < a_{2n-1}$ – isolated zeros of function $f(y)$, i. e. $f(a_i) = 0$. It is obviously that problem (1)–(2) has trivial solutions:

$$y = a_i, \quad i = 1, 2, \ldots, 2n-1. \tag{10}$$

Here $f(y)$ is a polynomial of odd degree, so it has odd number of zeros. The function (9) is negative on (a_1, a_2), then the function is positive on (a_2, a_3). Therefore, the function has n pairs of humps, where $f(y) > 0$ on (a_{2n-2}, a_{2n-1}) and $f(y) < 0$ on (a_{2n-3}, a_{2n-2}).

We suppose that $f(y)$ satisfies the conditions $F(a_1) < F(a_2) \ldots < F(a_{2n-2}) < F(a_{2n-1})$. Each solution branch has its maximal values inside a single positive hump, and, f. e., that it is necessary to have $\int_{a_1}^{a_3} f(y)\,dy > 0$ in order for solutions with maximal values in (a_2, a_3) to exist. Plots of functions $f(y)$ and $F(y)$ are depicted on Fig. 1.

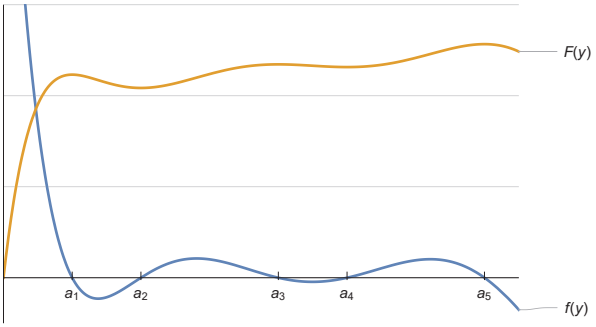


FIGURE 1. $f(y)$ and $F(y)$

Figure 2 shows a plot of the function (8) in the plane $(a; G(a))$, where f corresponds to (9). It follows from the plot that $G(a)$ has zeros only in the intervals (a_2, a_3), (a_4, a_5), $(a_6, a_7), \ldots, (a_{2n-2}, a_{2n-1})$ therefore only in these intervals

bifurcation points exist. Also it is clearly that function $G(a)$ exists only on the intervals where $f(y) > 0$.

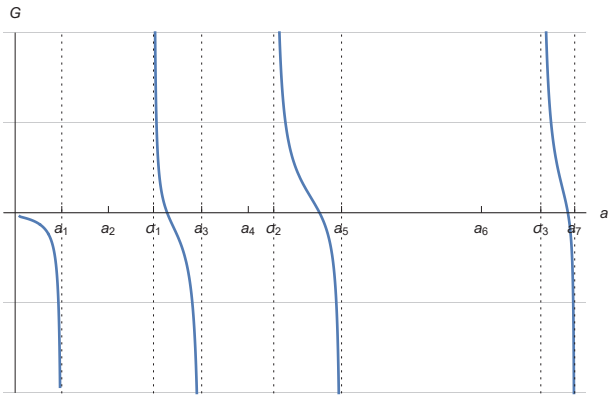


FIGURE 2. $G(a)$ for $f(y)$ - polynomial of odd degree

We will use the asymptotic behavior of $G(a)$ to make the intervals, where $G(a) = 0$, more precise:

1. $\lim\limits_{a \to a_{2n-1}^-} G(a) = -\infty$, i. e., to the left of a_{2n-1} there is no bifurcation point, where $n = 2, \ldots, k,\ k \geq 2$.

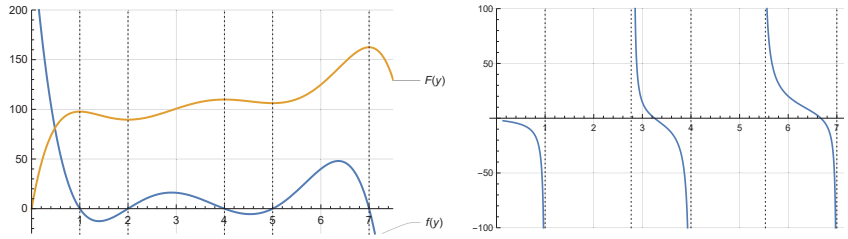
2. Let exist a point $\sigma_{n-1} \in (a_{2n-2}, a_{2n-1})$, such that $\int\limits_{a_{2n-3}}^{\sigma_{n-1}} f(s)\, ds = 0$, so $\lim\limits_{a \to \sigma_{n-1}^+} G(a) = +\infty$, i. e., to the right of σ_{n-1} there is no bifurcation point, where $n = 2, \ldots, k,\ k \geq 2$.

Polynomial of third degree (cubic) is well-studied in [4]. Authors show the existence of a critical value of the parameter $\lambda = \lambda_0$, so that for $0 < \lambda < \lambda_0$ the problem (3)–(4) with $f(y) = (y - a_1)(y - a_2)(a_3 - y)$ has exactly one solution, for $\lambda = \lambda_0$ it has exactly two solutions, and exactly three solutions for $\lambda > \lambda_0$.

Let consider the examples of polynomials of fifth and seventh degrees.

Example 1. Polynomial of 5th degree.

Let $f(y) = (y-1)(y-2)(y-4)(y-5)(7-y)$ [5]. First, we plot $f(y)$ and $F(y)$ (3(a)) and $G(a)$ (3(b)) to visualize their behavior. It follows from the plot of the function $G(a)$ that there are two bifurcation points on intervals (a_2, a_3), and (a_4, a_5), where $f(y) > 0$ (intervals $(2; 4)$ and $(5; 7)$). We plot a bifurcation diagram as it presented in formula (7) corresponding to this problem (Fig. 4).



(a) $f(y)$ and $F(y)$ (b) $G(a)$

FIGURE 3. Plots of $f(y)$, $F(y)$ and $G(a)$ for example 1

Using accurate commands NMinimize and FindRoot of Wolfram Mathematica we define turning points of $\lambda(a)$: $a_1 \approx 3.2417$, $a_2 \approx 6.5866$, where $\lambda_0 \approx 0.56973$ and $\lambda_1 \approx 0.6321$ (they are sorted in ascending order).

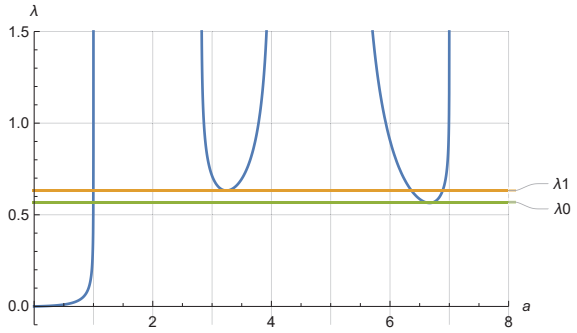
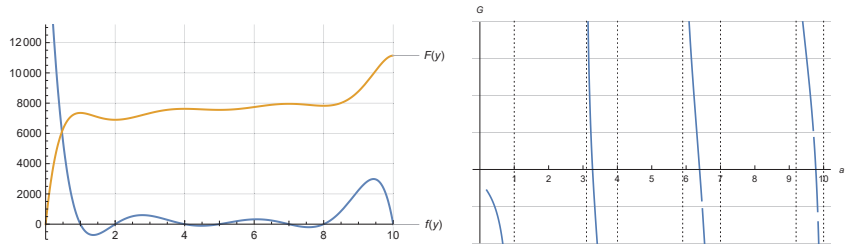


FIGURE 4. $\lambda(a)$ for problem in example 1

As we see on Fig. 4 there exists $0 < \lambda_0 < \lambda_1$ such that for $\lambda < \lambda_0$ there is one solution, $\lambda = \lambda_0$ there are two solutions, for $\lambda_0 < \lambda < \lambda_1$ there are three solutions, for $\lambda = \lambda_1$ there are four solutions and $\lambda > \lambda_1$ there are five solutions to the problem (1)–(2), where $f(y) = (y-1)(y-2)(y-4)(y-5)(7-y)$.

Example 2. Polynomial of 7th degree.
Let $f(y) = (y-1)(y-2)(y-4)(y-5)(y-7)(y-8)(10-y)$. Again we plot $f(y)$ and $F(y)$ (Fig. 5(a)) and $G(a)$ (Fig. 5(b)) to define the intervals where bifurcation points can occur. There are three bifurcation points, each on interval (a_2, a_3), (a_4, a_5) and (a_6, a_7), respectively. These intervals are $(2; 4)$, $(5; 7)$ and $(8; 10)$, where $f(y) > 0$. Bifurcation diagram for this problem is presented at Fig. 6. With the help of numeric computing methods of Wolfram Mathematica we define



(a) $f(y)$ and $F(y)$ (b) $G(a)$

FIGURE 5. Plots of $f(y)$, $F(y)$ and $G(a)$ for example 2

bifurcation points: $a_1 \approx 3.27276,\ a_2 \approx 6.38791,\ a_3 \approx= 9.6693$, where ordered by ascending values of λ are $\lambda_0 \approx 0,0181,\ \lambda_1 \approx 0.0194,\ \lambda_2 \approx 0.0633$.

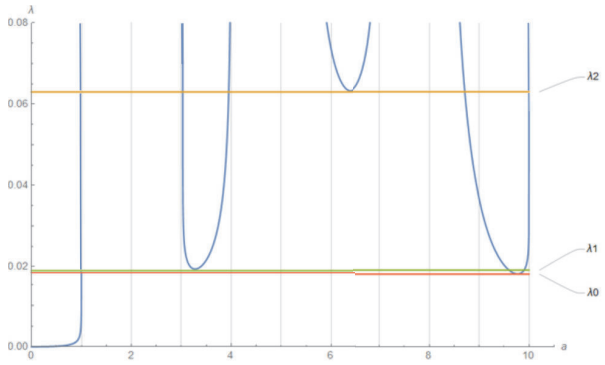


FIGURE 6. $\lambda(a)$ for problem in example 2

There exist $0 < \lambda_0 < \lambda_1 < \lambda_2$ such that for $\lambda < \lambda_0$ there is one solution to the problem, $\lambda = \lambda_0$ there are two solutions, for $\lambda_0 < \lambda < \lambda_1$ there are three solutions, for $\lambda = \lambda_1$ there are four solutions, $\lambda_1 < \lambda < \lambda_2$ there are five solutions, $\lambda = \lambda_2$ there are six solutions and $\lambda > \lambda_2$ there are seven solutions to the problem.

Conclusion

The obtained results generalize [5]. The study of the function $G(a)$ showed that it has zeros only in the intervals $(a_2, a_3),\ (a_4, a_5),\ (a_6, a_7), \ldots, (a_{2n-2}, a_{2n-1})$, where $f(y)$ – polynomial of odd degree ($f(a_i) = 0$), and consequently only these intervals contain bifurcation points. The odd degree of the polynomial $f(y)$ exactly determine the number of solutions of BVP (1)–(2). The bifurcation approach to

the problem assists to find out bifurcation parameters λ_i to understand when the number of solutions changes.

Computational methods of numerical integration and differentiation, as well as visualization of $G(a)$ and $\lambda(a)$ in the computing system Wofram Mathematica 11.0, have defined themselves as an effective tool for studying the function $G(a)$ from P. Korman, Y. Li and T. Ouyang Theorem, bifurcation curves and finding out the number of positive solutions of the problem.

References

[1] P. Korman, *Global Solution Branches and Exact Multiplicity of Solutions for Two Point Boundary Value Problems*. Handbook of Differential Equations: Ordinary Differential Equations, 2006.

[2] R. Schaaf, *Global Solution Branches of Two Point Boundary Value Problems*, Lecture Notes in Mathematics, Springer-Verlag, 1990.

[3] P. Korman, Y. Li, T. Ouyang *Computing the location and the direction of bifurcation*, Math. Research Letters, 2005.

[4] P. Korman, Y. Li, T. Ouyang *Exact multiplicity results for boundary value problems with nonlinearities generalising cubic*, Proc. Royal Soc. Edinburgh, 1996.

[5] P. Korman, Y. Li, T. Ouyang *Verification of bifurcation diagrams for polynomial-like equations*, Journal of Computational and Applied Mathematics, 2008.

Daria Chemkaeva
Dep. of Informatics & Technology
Herzen State Pedagogical University
St.Petersburg, Russia
e-mail: dariachemkaeva@yahoo.com

Alexandr Flegontov
Dep. of Informatics & Technology
Herzen State Pedagogical University
St.Petersburg, Russia
e-mail: flegontoff@yandex.ru

A New Approach to Effective Computation of the Dimension of an Algebraic Variety

Alexander L. Chistov

Abstract. We discuss a new method for computing the dimension of an algebraic variety. It is based on the effective version of the first Bertini theorem for hypersurfaces suggested by the author earlier.

Computation of the dimension of an algebraic variety is a classical problem in effective algebraic geometry. In the most simple case it is formulated as follows. Let k be a field with the algebraic closure $\overline{k}$. Given homogeneous polynomials $f_1, \ldots, f_m \in k[X_0, \ldots, X_n]$ the problem is to compute the dimension of the algebraic variety $\mathcal{Z}(f_1, \ldots, f_m)$ of all the common zeroes of the polynomials $f_1, \ldots, f_m$ in the projective space $\mathbb{P}^n(\overline{k})$.

Assume additionally that the degrees $\deg_{X_0,\ldots,X_n} f_j \leqslant d$ for an integer $d \geqslant 2$ for all $1 \leqslant i \leqslant m$. Then the number of coefficients of each polynomial f_j is at most $\binom{n+d}{n}$. So it is bounded from above by a polynomial in d^n.

On the other hand, one can verify whether the set $\mathcal{Z}(f_1, \ldots, f_m)$ is finite (or empty) and if $\#\mathcal{Z}(f_1, \ldots, f_m) < +\infty$ solve the homogeneous system $f_1 = \ldots = f_m = 0$ over the algebraically closed field $\overline{k}$. The complexity of this algorithm is polynomial in d^n and the size of the input data, see [4]. Actually the main ideas for solving homogeneous systems of polynomial equations with a finite number of roots are classical and were known at the beginning of the previous century, see [5].

Let us return to the general case. Now the probabilistic algorithm for computing the dimension of an algebraic variety is simple. Let s be an integer such that $-1 \leqslant s \leqslant n$. Let us choose linear forms $L_0, \ldots, L_s \in k[X_0, \ldots, X_n]$ randomly. Then the dimension $\dim \mathcal{Z}(f_1, \ldots, f_m)$ is the least s such that the set

$$\mathcal{Z}(f_1, \ldots, f_m, L_0, L_1, \ldots, L_s)$$

is empty. So one can compute the dimension of a projective algebraic variety probabilistically within the time polynomial in d^n and the size of the input data.

But to compute the dimension deterministically is much more difficult. In the case of arbitrary characteristic it is an open problem

(*) to construct a deterministic algorithm for computing the dimension of a projective algebraic variety $\mathcal{Z}(f_1, \ldots, f_m)$ with bitwise complexity polynomial in d^n and the size of the input data.

We think that for arbitrary characteristic of the ground field this problem will not be solved in near future (say, in this century).

Still here there have been a major progress. In the case of the ground field of zero–characteristic we solved the problem (*), see [1]. We could obtain the main result of [1] using the methods of real algebraic geometry. After that we have developed the whole theory basing on these methods and get many important results. However, to many specialists it seemed unnatural to apply the methods of real algebraic geometry for varieties over algebraically closed fields. On the other hand, it is a fact that all other attempts to compute the dimension deterministically within the time polynomial in d^n and the size of the input data have been fruitless.

The situation has changed after the results of [2]. Namely, in [2] we got a very strong and explicit version of the first Bertini theorem for the case of a hypersurface. Now it is possible to attract the new ideas related to irreducibility and transversality of intersections of algebraic varieties. Quite probably (one should check the details) that in the case of the ground field of zero–characteristic one can solve the problem (*) with the help of [2] (and without using methods of real algebraic geometry).

These techniques are not sufficient for the case of the ground field of nonzero characteristic. Here the main difficulties are related to inseparability. But the situation is not so hopeless. In the case of nonzero characteristic one can use additionally the results [3]. We would like to formulate the following hypothesis.

(†) In the case on nonzero characteristic one can one construct a deterministic algorithm for computing the dimension of a projective algebraic variety $\mathcal{Z}(f_1, \ldots, f_m)$ with bitwise complexity polynomial in $C(n)d^n$ and the size of the input data where the constant $C(n)$ depends only on n (more precisely, $C(n) < 2^{2^{n^C}}$ for an absolute constant $C > 0$, cf. [3]).

References

[1] A.L. Chistov, *Polynomial-time computation of the dimension of algebraic varieties in zero-characteristic*, Journal of Symbolic Computation. 1996, v.22, # 1, p. 1–25.

[2] A.L. Chistov, *A bound for the degree of a system of equations determining the variety of reducible polynomials*. Algebra i Analiz , v. 24 (2012), No. 3, p. 199-222 (in Russian) [English translation: St.Petersburg Math. J., v.24 (2013), # 3, p. 513–528].

[3] A.L. Chistov, *Efficient construction of local parameters for irreducible components of an algebraic variety in nonzero characteristic*, Zapiski Nauchnyh Seminarov POMI v. 326 (2005) p. 248-278 (in Russian) [English translation: Journal of Mathematical Sciences v.140 (2007), # 3, p. 480–496].

[4] D.Lazard *Résolution des systémes d'équations algébriques*, Theor. Comput. Sci. v.15 (1981), p. 77–110.

[5] F.S. Macauley, *The algebraic theory of modular systems*, Cambridge University Press, 1916.

Alexander L. Chistov
St. Petersburg Department of Steklov Mathematical Institute
of the Academy of Sciences of Russia
Fontanka 27, St. Petersburg 191023, Russia
e-mail: alch@pdmi.ras.ru

Computer assisted constructive tasks with infinite set of solutions for mathematical olympiads and contests

Chukhnov, A. S., Posov, I. A.; and Pozdniakov S. N.

Abstract. The report presents a usage experience of constructive educational tasks based on computer models. It is shown, that participants of competitions may construct many and various different solutions if they use software tools based on a computer model of a subject field to manipulate its objects. A solution representation in terms of some construction allows for assessing this solution by means of a set of formal criteria. Some criteria may be specified explicitly as objective functions to be optimized by participants, others may be stated a posteriori to test different methodological hypothesis about solutions features.

From the point of view of automatic assessment, this approach can be treated as a transition from multiple choice tests to tasks with an infinite set of solutions. To specify a way to automatically asses a constructive solution, a teacher does not need to describe a solution that he or she should know in advance. He or she should rather specify a set of criteria that must hold for a solution. Criteria used to analyze a solution also allow for assessing partial solutions and providing feedback for participants while they work with a task and thus adjust their work.

Authors also explore a usage of constructive tasks uas an intermediate step to generalize partial solutions and ideas to justify the full solution. The series of competitions in discrete mathematics have been designed and implemented. This competitions suppose a constructive activity with software tools to be followed by theoretical tasks. Such series of tasks were also tried out as a part of the discrete mathematics course in a technical university.

During the experiments held inside the „Construct, Test, Explore" competition and inside the Olympiad in discrete mathematics and computer science, the constructive tasks proved to be appropriate for participant of different level of preparation. But they also proved to have a drawback, that participants overfocused on the experimental activity to the expense of theoretical analysis of a task.

The work was supported by the Russian Foundation for Basic Research (Project No. 18-013-01130).

2

Chukhnov, A. S.
Department of higher mathematics 2
Saint Petersburg Electrotechnical University „LETI”
Saint Petersburg, Russia
e-mail: septembreange@gmail.com

Posov, I. A.;
Department of information systems in arts and humanities
Saint Petersburg State University
Saint Petersburg, Russia
Department of higher mathematics 2
Saint Petersburg Electrotechnical University „LETI”
Saint Petersburg, Russia
e-mail: iposov@gmail.com

Pozdniakov S. N.
Department of higher mathematics 2
Saint Petersburg Electrotechnical University „LETI”
Saint Petersburg, Russia
e-mail: pozdnkov@gmail.com

Schutzenberger transformation on graded graphs: Implementation and numerical experiments.

Vasilii Duzhin and Nikolay Vassiliev

1. Introduction

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

The connection between Schutzenberger transformation, RSK correspondence [3, 4, 5] and Markov Plancherel process [7] was found in [6]. The techniques discussed in the work [6] have been developed in the recently published paper [8].

We consider the Schutzenberger transformation on two- and three- dimensional Young tableaux. The Schutzenberger transformation converts a Young tableau of size n to another Young tableau of size $n-1$. At the beginning, the first box of a source tableau is being removed. Then, the box with a smaller number is being selected among top neighbouring and right neighbouring boxes. The selected box is then being shifted to the position of the removed box. A newly formed empty box is being filled by the neighbouring box using the same rule. This process continues until the front of the diagram is reached.

The sequence of the shifted boxes forms so-called jeu de taquin path [8] or *Schutzenberger path*. Schutzenberger path is a path in Pascal graphs: $\mathbb{Z}^2_+$ or $\mathbb{Z}^3_+$ in 2D and 3D cases, respectively.

Besides the classic Schutzenberger transformation, in this work we also consider two different modifications of it. In the first modification, we add an extra box in the position of the last shifted box. In this case, the Schutzenberger transformation does not change the shape of a diagram. Also the transformation becomes reversible, i.e. it establishes a bijection on the paths to a diagram. The second modification is a randomization of the classic Schutzenberger transformation. In

This work was supported by grant RFBR 17-01-00433.

this case a path to a diagram on the third level of Young graph is being selected randomly. The results of numerical experiments suggest that the iterations of the randomized Schutzenberger transformation generate uniform distribution on the paths to a diagram.

A. M. Vershik has noticed that the Schutzenberger algorithm can be applied not only to the Young tableaux of an arbitrary dimension, but generally to any partially ordered set. In this case the Schutzenberger transformation works on ascendant sequences of decreasing ideals of a corresponding poset. Particularly, the technique of the Schutzenberger transformation can be used on any graded graph. In this situation, a Schutzenberger path will be a path on this graded graph.

It was proved in [8] that the Schutzenberger paths, obtained on two-dimensional Young tableaux, have a certain limit angle with a probability 1 relatively to the Plancherel measure.

Note that the standard Schutzenberger transformation is not reversible. Wherein each Young tableau has as many preimages as the number of transitions from a given diagram of size n to the level $n+1$. Fig. 1 shows the Schutzenberger paths of all preimages of the 2D Young tableau of size 10^6.

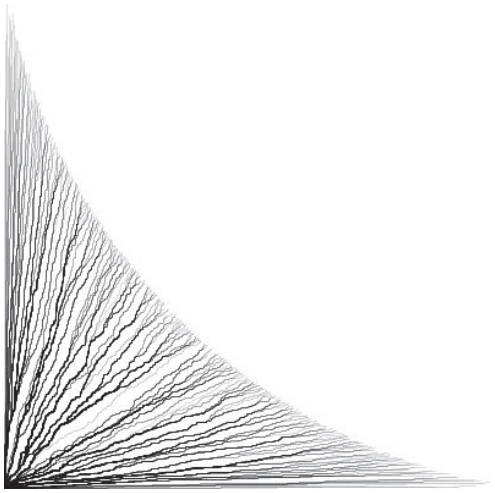


FIGURE 1. The Schutzenberger paths of all preimages of the Young tableau of size 10^6.

1.1. The implementation of the Schutzenberger transformation

We propose the following algorithm for the implementation of the Schutzenberger transformation on 2D and 3D Young tableaux. The same algorithm with minor modifications can be applied to any graded graph. We present Young tableaux as

arrays of sets of coordinates of added boxes. Note that the standard presentation of Young tableaux as two-dimensional arrays of integers has a significant disadvantage with respect to the computational cost and memory usage. That is because in that case the Schutzenberger transformation requires renumbering of all boxes in a tableau.

Let us consider the implemented algorithm for the case of 2D Young tableaux. During operation of the algorithm, the coordinates of boxes of a source tableau are processed consequently. At the beginning, the first box of a source tableau with coordinates (0,0) is assigned as an *active* box. However, the active box is not being added to a new tableau immediately.

The active box is being added to a new tableau at the moment when a neighbour top or neighbour right box is added to a source tableau. As a next step, this neighbour box becomes active and so on. At the same time, the non-neighbour boxes are being added without any delay. The algorithm stops when all the boxes in a source tableau are processed.

Note that during operation of the algorithm, most of the boxes of a source table are being copied to a new tableau without any changes. Only the order of addings of active boxes will be different. Another advantage of this approach is that after necessary modifications it can be easily implemented on a Young graph of any dimension and on any other graded graphs.

We use the same methods to implement the modifications of Schutzenberger transformation, i.e. the Schutzenberger transformation with the preservation of shape of a diagram and with randomization. The fragment of the algorithm of Schutzenberger transformation in 2D case, written in pseudocode, is shown below. Note that $actX, actY$ are the coordinates of the current active box, in_tab is a source tableau and out_tab is a transformed tableau.

Listing 1. Schutzenberger transformation on 2D Young tableaux

```
1  actX = 0; actY = 0;
2  for each (x,y) from in_tab:
3  {
4      if ((x == actX + 1) && (y == actY)) ||
5         ((x == actX)     && (y == actY + 1))
6      {
7          out_tab.add(actX,actY);
8          actX = x; actY = y;
9      }
10     else
11     {
12         out_tab.add(x,y);
13     }
14 }
15 out_tab.add(actX,actY);
```

2. Numerical experiments

Here we discuss the numerical experiments where the Schutzenberger transformation was applied on large 2D and 3D Young tableaux. Particularly, we have generated a 2D random Plancherel Young tableau of 3 million boxes. The Schutzenberger transformation with the preservation of shape was consequently applied to this tableau. The Vershik-Kerov coordinates $\frac{x+y}{\sqrt{3\cdot 10^6}}$ of the last boxes (x,y) of Schutzenberger paths were recorded. The distribution of these coordinates is shown in Fig. 2.

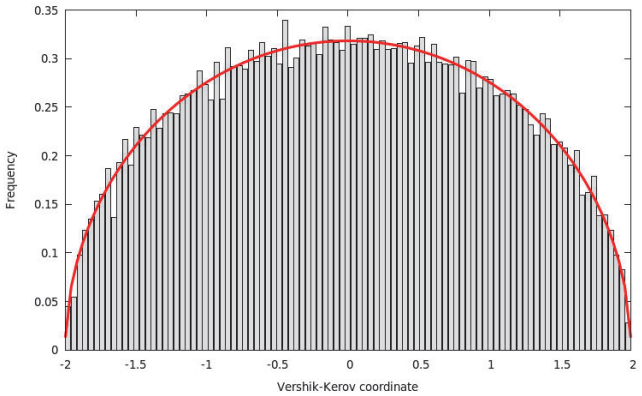


FIGURE 2. The histogram of frequencies of last boxes of Schutzenberger paths of 2D Young tableaux.

It can be seen from the figure that this histogram has the shape of so-called semicircle distribution. The same distribution was obtained in [9] as a limit distribution of Plancherel probabilities on the front of large Young diagrams of size $n, n \to \infty$. It has the following density function:

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

where u is one of Vershik-Kerov coordinates: $u = \frac{x-y}{\sqrt{n}}$.

The next numerical experiment is devoted to the Schutzenberger transformation on 3D Young graph. For each iteration of the Schutzenberger transformation we compute the coordinates of the last boxes of Schutzenberger paths on the front of random Young tableaux of a fixed shape. The distribution of the coordinates obtained in this experiment is shown in Fig. 3. Note that the size of the corresponding tableau is 3 million boxes.

As we can see, the distribution of last boxes of 3D Schutzenberger paths on the front of the diagram is close to uniform. We plan to conduct more numerical experiments to investigate this 3D distribution more precisely.

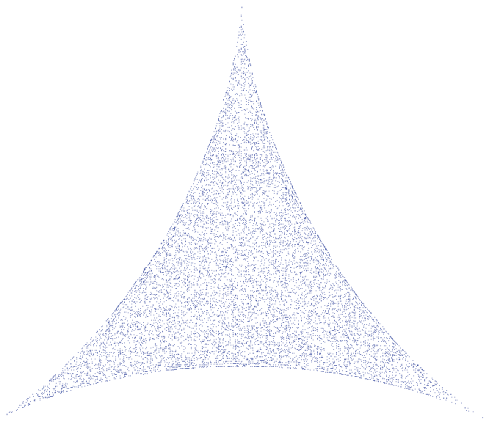


FIGURE 3. The distribution of coordinates of last boxes of Schutzenberger paths of 3D Young tableaux.

Also we used the randomized Schutzenberger transformation to calculate the ratio of dimensions of a pair of three-dimensional Young diagrams of sizes n and $n+1$ which differ in a single box, i. e. a pair of diagrams connected with an edge in the Young graph. The co-transition probabilities of 3D central processes can be obtained using such ratios. The Schutzenberger transformation gives us these co-transition probabilities without calculating the exact dimensions. That is especially useful because there are no known three-dimensional analog of the 2D hook length formula.

References

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

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

[3] G. de B. Robinson, "On the representations of the symmetric group", *American Journal of Math.* 60, (1938), 745-760.

[4] C. Schensted, "Longest increasing and decreasing subsequences", *Canadian Journal of Math.* 13, (1961), 179-191.

[5] Donald E. Knuth. Permutations, matrices, and generalized Young tableaux. *Pacific J. Math.* Volume 34, Number 3 (1970), pp. 709-727.

[6] Sergei V. Kerov and Anatol M. Vershik. The characters of the infinite symmetric group and probability properties of the Robinson-Schensted-Knuth algorithm. *SIAM J. Algebraic Discrete Methods*, 7(1):116–124, 1986

[7] S.V.Kerov and A.M.Vershik. Asymptotics of the Plancherel measure of the symmetric group and the limiting form of Young tableaux. *Dokl. Akad. Nauk SSSR* 233, No.6, 1024-1027 (1977).
English translation: Sov. Math. Dokl. 18, 527-531 (1977).

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

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

Vasilii Duzhin
Saint Petersburg Electrotechnical University
ul. Professora Popova 5, 197376 St. Petersburg, Russian Federation
e-mail: vduzhin.science@gmail.com

Nikolay Vassiliev
St.Petersburg department of Steklov Institute of mathematics RAS
nab.Fontanki 27,St.Petersburg, 191023, Russia
e-mail: vasiliev@pdmi.ras.ru

Local and Global Integrability of ODEs

Victor Edneral and Valery Romanovski

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

Full Phase Space Integrability

Firstly we studied the system which is a partial case of the system[4]

$$\begin{aligned} \frac{dx}{dt} &= -y^3 - b\,x^3y + a_0\,x^5 + a_1\,x^2y^2, \\ \frac{dy}{dt} &= \frac{1}{b}\,x^2y^2 + x^5 + b_0\,x^4y + b_1\,x\,y^3. \end{aligned} \tag{1}$$

Thus, we consider the system with five arbitrary parameters a_i, b_i, $(i = 0, 1)$ and $b \neq 0$. After the power transformation

$$x = u\,v^2, \qquad y = u\,v^3,$$

we obtained the system in the form

$$\begin{aligned}\frac{du}{d\tau} &= -3\,u - [3\,b + (2/b)]u^2 - 2\,u^3 + (3\,a_1 - 2\,b_1)u^2 v + (3\,a_0 - 2\,b_0)u^3 v\,,\\ \frac{dv}{d\tau} &= v + \left[b + \frac{1}{b}\right] u\,v + u^2 v + (b_1 - a_1)u\,v^2 + (b_0 - a_0)u^2 v^2\,.\end{aligned} \tag{2}$$

The point $x = y = 0$ blows up into two straight invariant lines $u = 0$ and $v = 0$. Along the line $u = 0$, the system has the stationary point $u = v = 0$. Along the second line $v = 0$. So if $b^2 \neq 2/3$, this system has four elementary stationary points[6]

$$u = 0, \qquad u = -\frac{1}{b}, \qquad u = -\frac{3b}{2}, \qquad u = \infty\,.$$

At the each point above there exist values of parameters when the system is locally integrable, but if $b^2 \neq 2/3$ there are only 4 two dimensional combinations, where local integrability takes place simultaneously

$$\begin{array}{llll} 1) & a_0 = 0, \quad a_1 = -b_0\,b, & b_1 = 0, & \\ 2) & b_1 = -2\,a_1, & a_0 = a_1 b, & b_0 = b_1 b, \\ 3) & b_1 = (3/2)\,a_1, & a_0 = a_1 b, & b_0 = b_1 b, \\ 4) & b_1 = (8/3)\,a_1, & a_0 = a_1 b, & b_0 = b_1 b. \end{array} \tag{3}$$

In [7], we have calculated first integrals of the system (2) for all cases (3) (mainly by the Darboux method, see, e.g., [8]). These integrals are

$I_1(x,y) = 2\,x^3 + 3\,b\,y^2,$
$I_2(x,y) = 2\,x^3 - 6\,a_1\,b\,x^2\,y + 3\,b\,y^2,$

$$I_3(x,y) = \frac{a_1 x^2 \left(-4 + 3^{5/6}\,{}_2F_1\left(2/3, 1/6; 5/3; -2\,x^3/(3\,b\,y^2)\right) \times \left(3 + 2x^3/(b\,y^2)\right)^{1/6}\right)}{y^{4/3}(3\,b + 2\,x^3/y^2)^{1/6}} + \frac{4y}{y^{4/3}(3\,b + 2\,x^3/y^2)^{1/6}},$$

$$I_4(u,v) = \frac{u\,(3 + 2\,a_1^2 b u) + 6\,a_1\,b\,v}{3\,u\left[u^3(6 + a_1^2 b\,u) + 6\,a_1^2 b\,u^2 v + 9\,b\,v^2\right]^{1/6}} - 8\,a_1\sqrt{-b}/3^{5/3} B_{6 + a_1\sqrt{-6\,b\,u} + 3\,v\sqrt{-6\,b/u^3}}(5/6, 5/6)\,,$$

where $B_t(a,b)$ is the incomplete beta function and ${}_2F_1(a,b;c;z)$ is the hypergeometric function [9].

In the case $b^2 = 2/3$ the situation is a bit more complicate and we have at least two additional stationary points which are compatible with (3) at $b^2 = 2/3$
5. $b_1 = 3a_1/2, \quad a_0 = (2b_0 + b(3a_1 - 2b_1))/3,$
6. $b_1 = 6a_1 + 2\sqrt{6}b_0, \quad a_0 = (2b_0 + b(3a_1 - 2b_1))/3,$ and two more global first

integrals of a motion for these values of parameters exist

$$I_5(x,y) = \frac{y}{x^2}\left(\sqrt{6}+\frac{2x^3}{y^2}\right)^{-7/6}\left(\frac{x^3}{y^2}\right)^{2/3}\times\Big\{42\sqrt{6}+\frac{1}{xy^3}\Big[-36a_1x^6-16\sqrt{6}b_0x^6 + 84x^4y-24\sqrt{6}a_1x^3y^2-36b_0x^3y^2+2^{1/3}\left(\frac{x^3}{y^2}\right)^{1/3}y^2\cdot\left(\sqrt{6}+\left(\frac{x^3}{y^2}\right)^{2/3}\right)\times \big(2\big(9a_1+4\sqrt{6}b_0\big)x^3+3\big(3\sqrt{6}a_1+8b_0\big)y^2\big)\times {}_2F_1\left(-1/2,1/3;1/2;\tfrac{3y^2}{3y^2+\sqrt{6}x^3}\right)\Big]\Big\},$$

$$I_6(x,y) = y\cdot\left(\sqrt{2/3}+\frac{x^3}{y^2}\right)^{-\frac{1}{2}+\frac{a_1}{-6a_1-2\sqrt{6}b_0}}\left(\frac{x^2}{y}\right)^{-\frac{a_1}{3a_1+\sqrt{6}b_0}}\times \left\{3+\frac{x^2}{y^2}\left[\sqrt{6}x+3\left(2a_1+\sqrt{6}b_0\right)y\right]\right\}.$$

Partial Phase Space integrability

We have examples when integrability takes place only in a part of the phase space. Let us see as the system

$$\begin{aligned}\frac{dx}{dt} &= \quad y+2xy,\\ \frac{dy}{dt} &= -\quad x-bx^2+cxy+y^2.\end{aligned}\tag{4}$$

This system has 3 different stationary points

$$\begin{aligned}&x=0, y=0,\\ &x=-(1/b), y=0,\\ &x=-1/2, y=(c-\sqrt{-4b-c^2-7})/4.\end{aligned}$$

The local integrability (i.e the center case) take place in the first case at $b=1$ or $c=0$ only. At this values the second and third cases are local nonintegrable cases (focuses), at that the third case lies in complex values of y. The corresponding first integrals are

$$\begin{aligned}&\text{At } b=1; \quad I(x,y)=(1+2x)(\frac{1}{4}(-4+c(c+\sqrt{c^2-4})),\\ &\text{At } c=0; \quad I(x,y)=(-1-2bx(1+x)-2y^2+(b-1)(2x+1)\log 2x+1)/(8x+4).\end{aligned}\tag{5}$$

In both cases we have the invariant line $x=-1/2$ which separates the left part, where exists the global first integral (center case) from right part side where integrability does not exist.

Conclusion

We propose the hypothesis that the local integrability in all stationary points of autonomous planar systems of ordinary differential equations with polynomial right

sides and resolved with respect to derivatives leads to existence of the global first integral if this system has these local integrability at the same sets of parameters. If the system has invariant curves or separatrices such integral can exist only in a part of the phase space.

Acknowledgements

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

References

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

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

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

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

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

[6] V.F. Edneral, *Application of Power Geometry and Normal Form Methods to the Study of Nonlinear ODEs*, EPJ Web of Conferences, v. 173, pp. 01004

[7] V.F. Edneral and V.G. Romanovski, *On Sufficient Conditions for Integrability of a Planar System of ODEs Near Degenerate Stationary Point*,LNCS 6244, Springer, Heidelberg, (2010) 97–105

[8] V.G. Romanovski and D.S. Shafer, *The Center and Cyclicity Problems: A Computational Algebra Approach*, Birkhäuser, Boston, (2009) 330 pp.

[9] H. Bateman and A. Erdélyi, *Higher Transcendental Functions, volume I*, McGraw-Hill Book Comp., New York, Toronto, London, (1953) p 316.

Victor Edneral
Skobeltsyn Institute of Nuclear Physics,
Lomonosov Moscow State University
Leninskie Gory 1(2), Moscow, 119991

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

e-mail: edneral@theory.sinp.msu.ru
e-mail: edneral_vf@pfur.ru

Valery Romanovski
Faculty of Electrical Engineering and Computer Science, University of Maribor, Koroška cesta 46, Maribor, SI-2000 Maribor,

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

Faculty of Natural Science and Mathematics, University of Maribor
Koroška cesta 160, SI-2000 Maribor, Slovenia

e-mail: valery.romanovsky@uni-mb.si

Thomas decomposition of differential systems and its implementation in Maple

Vladimir Gerdt, Markus Lange-Hegermann and Daniel Robertz

We present the basic algorithmic features and implementation in Maple of the differential Thomas decomposition of polynomially nonlinear differential systems, which in addition to equations may contain inequations, into a finite set of differentially triangular and algebraically simple subsystems whose subsets of equations are involutive. Usually the decomposed system is substantially easier to investigate and solve both analytically and numerically. The distinctive property of a Thomas decomposition is disjointness of the solution sets of the output subsystems. Thereby, a solution of a well-posed initial problem belongs to one and only one output subsystem. The Thomas decomposition is fully algorithmic. It allows to perform important elements of algebraic analysis of an input differential system such as: verifying consistency, i.e., the existence of solutions; detecting the arbitrariness in the general analytic solution; given an additional equation, checking whether this equation is satisfied by all common solutions of the input system; eliminating a part of dependent variables from the system if such elimination is possible; revealing hidden constraints on dependent variables, etc. Examples illustrating the use of the differential Thomas decomposition are given.

References

[1] Thomas Bächler, Vladimir Gerdt, Markus Lange-Hegermann and Daniel Robertz. *Algorithmic Thomas decomposition of algebraic and differential systems*. Journal of Symbolic Computation 47(10), 1233–1266, 2012.

[2] Daniel Robertz. *Formal Algorithmic Elimination for PDEs*. Lecture Notes in Mathematics, Vol. 2121, Springer, 2014.

[3] Vladimir Gerdt, Markus Lange-Hegermann and Daniel Robertz. *The MAPLE package TDDS for computing Thomas decompositions of systems of nonlinear PDEs*. arXiv:1801.09942 [physics.comp-ph]

Vladimir Gerdt
Laboratory of Information Technologies
Joint Institute for Nuclear Research
141980 Dubna, Russia
e-mail: gerdt@jinr.ru

Markus Lange-Hegermann
University of Applied Science Ostwestfalen-Lippe
32656 Lemgo, Germany
e-mail: markus.lange-hegermann@hs-owl.de

Daniel Robertz
School of Computing, Electronics and Mathematics
Plymouth University
PL4 8AA Plymouth, United Kingdom
e-mail: daniel.robertz@plymouth.ac.uk

Upper bounds on Betti numbers of tropical prevarieties

Dima Grigoriev and Nicolai Vorobjov

We prove upper bounds on the sum of Betti numbers of tropical prevarieties in dense and sparse settings. In the dense setting the bound is in terms of the volume of Minkowski sum of Newton polytopes of defining tropical polynomials, or, alternatively, via the maximal degree of these polynomials. In sparse setting, the bound involves the number of the monomials.

Dima Grigoriev
French National Center for Scientific Research
3, rue Michel-Ange
75794 Paris cedex 16
France
e-mail: dima.grigoryev@gmail.com

Nicolai Vorobjov
University of Bath
Claverton Down
Bath
BA2 7AY
United Kingdom
e-mail: nnv@cs.bath.ac.uk

Double Hurwitz Numbers

Maksim Karev

Abstract. The talk is based on the joint work with N. Do (Monash University). The most straightforward definition of the double Hurwitz numbers $D_g(\mu, \nu)$ is, up to a multiplicative constant, the number of ways to multiply a given permutation of cyclic type μ by a product of $2g - 2 + |\mu| + |\nu|$ transpositions such that the result is of cyclic type ν. It turns out that these number can be packed into generating functions that can be calculated using a recursion. We formulate a conjecture on the analytical properties of these generating functions.

Introduction

The talk is based on the joint work with N. Do (Monash University). Simple Hurwitz numbers enumerate the number of ways to decompose a permutation of a given cyclic type into a product of fixed number of transpositions. Their study was first initiated in nineteenth century by A. Hurwitz. However, they still attract the interest due to incredibly rich structure they possess.

Double Hurwitz numbers are defined in a similar way: we fix two cyclic type μ and ν in the symmetric group S_d and count the number of ways to multiply a permutation of a cyclic type μ by a product of $2g - 2 + |\mu| + |\nu|$ transpositions such that the result is of cyclic type ν.

It is well-known that both simple and double Hurwitz numbers can be interpreted as a number of non-isomorphic ramified covers of $\mathbb{C}P^1$ with certain restriction on the branch points profiles. It allows us to compute double Hurwitz numbers via the enumeration of ramified covers weighted by a certain polynomial weight as follows.

Fix a positive integer d and weights $s, q_1, q_2, \ldots, q_d \in \mathbb{C}$. Define the *double Hurwitz number* $DH_{g,n}(\mu_1, \ldots, \mu_n)$ to be the weighted count of connected genus g branched covers of the Riemann sphere $f : (\Sigma; p_1, \ldots, p_n) \to (\mathbb{CP}^1; \infty)$ such that

- all branching away from 0 and ∞ is simple and occurs at some number m of fixed points;

- $f^{-1}(\infty) = \mu_1 p_1 + \cdots + \mu_n p_n$; and
- no preimage of 0 has ramification index larger than d.

If such a branched cover has ramification profile $(\lambda_1, \lambda_2, \ldots, \lambda_\ell)$ over 0, then we assign it the weight

$$\frac{q_{\lambda_1} q_{\lambda_2} \cdots q_{\lambda_\ell}}{|\mathrm{Aut}\ f|} \frac{s^m}{m!}.$$

Here, the automorphism group Aut f consists of Riemann surface automorphisms $\phi : \Sigma \to \Sigma$ that preserve the marked points $p_1, \ldots, p_n$ and satisfy $f \circ \phi = f$.

We present an efficient recursion that, in principle, allows to compute all double Hurwitz numbers, and formulate an explicit conjecture concerning the properties of the corresponding generating functions.

Maksim Karev
Representation theory and dynamical systems laboratory
PDMI RAS
St Petersburg, Russia
e-mail: max.karev@gmail.com

Irreducible Decomposition of Representations of Finite Groups via Polynomial Computer Algebra

Vladimir V. Kornyak

Abstract. An algorithm for splitting permutation representations of finite group over fields of characteristic zero into irreducible components is described. The algorithm is based on the fact that the components of the invariant inner product in invariant subspaces are operators of projection into these subspaces. An important part of the algorithm is the solution of systems of quadratic equations. A preliminary implementation of the algorithm splits representations up to hundreds of thousands of dimensions. Examples of computations are given.

1. Introduction. One of the central problems of group theory and its applications in physics is the decomposition of linear representations of groups into irreducible components. In general, the problem of splitting a module over an associative algebra into irreducible submodules is quite nontrivial. An overview of the algorithmic aspects of this problem can be found in [1]. For vector spaces over finite fields, the most efficient is the Las Vegas type algorithm called *MeatAxe*. This algorithm played an important role in solving the problem of classifying finite simple groups. However, the approach used in the *MeatAxe* is ineffective in characteristic zero, whereas quantum-mechanical problems are formulated just in Hilbert spaces over fields of characteristic zero. Our algorithm deals with representations over such fields, and its implementation copes with dimensions up to hundreds of thousands that is not less than the dimensions achievable for the *MeatAxe*. The algorithm requires knowledge of the centralizer ring of the considered group representation. In the general case, the calculation of the centralizer ring is a problem of linear algebra, namely, solving matrix equations of the form $AX = XA$. In the case of permutation representations, there is an efficient algorithm for computing the centralizer ring — it is reduced to constructing the set of orbitals. In addition, permutation representations are fundamental in the sense that any linear representation of a finite group is a subrepresentation of some permutation representation, and we use this fact in some quantum mechanical considerations [2, 3]. Therefore, we consider here only permutation representations.

2. Mathematical preliminaries. Let G be a *transitive* permutation group on the set $\Omega \cong \{1, \ldots, \mathsf{N}\}$. The action of $g \in \mathsf{G}$ on $i \in \Omega$ is denoted by i^g. A representation of G in an N-dimensional vector space over a field $\mathcal{F}$ by the matrices $\mathrm{P}(g)$ with the entries $\mathrm{P}(g)_{ij} = \delta_{ig\,j}$, where δ_{ij} is the Kronecker delta, is called a *permutation representation*. We assume that the permutation representation space is a Hilbert space $\mathcal{H}_{\mathsf{N}}$. From a constructive point of view it is sufficient to assume that the

base field $\mathcal{F}$ is a *minimal splitting field* of the group G. Such field is a subfield of an m-th cyclotomic field, where m is a divisor of the *exponent* of G. The field $\mathcal{F}$, being an abelian extension of $\mathbb{Q}$, is a constructive dense subfield of $\mathbb{R}$ or $\mathbb{C}$.

An orbit of G on the Cartesian square $\Omega \times \Omega$ is called an *orbital* [5]. The number of orbitals, R, is called the *rank* of G on Ω. Among the orbitals of a transitive group there is one *diagonal* orbital, $\Delta_1 = \{(i,i) \mid i \in \Omega\}$, which will always be fixed as the first element in the list of orbitals $\Delta_1, \ldots, \Delta_{\mathrm{R}}$. For a transitive action of G there is a natural one-to-one correspondence between the orbitals of G and the orbits of a point stabilizer G_i: $\Delta \longleftrightarrow \Sigma_i = \{j \in \Omega \mid (i,j) \in \Delta\}$. The G_i-orbits are called *suborbits* and their cardinalities are called the *suborbit lengths*.

The invariance condition for a bilinear form A in the Hilbert space $\mathcal{H}_{\mathsf{N}}$ can be written as the system of equations $A = \mathrm{P}(g)\, A \mathrm{P}\big(g^{-1}\big)\,,\ g \in \mathsf{G}$. It is easy to verify that in terms of the entries the equations of this system have the form $(A)_{ij} = (A)_{i^g j^g}$. Thus, the matrices $\mathcal{A}_1, \ldots, \mathcal{A}_{\mathrm{R}}$, where $\mathcal{A}_r$ is the characteristic function of the orbital Δ_r on the set $\Omega \times \Omega$, form a *basis* of the *centralizer ring* of the representation P. The *multiplication table* for this basis has the form $\mathcal{A}_p \mathcal{A}_q = \sum_{r=1}^{\mathrm{R}} C^r_{pq} \mathcal{A}_r$, where C^r_{pq} are non-negative integers. The commutativity of the centralizer ring indicates that the representation P is *multiplicity-free*.

3. Algorithm and its implementation. Let T be a transformation (we can assume that T is unitary) that splits the permutation representation P into M irreducible components:

$$T^{-1}\mathrm{P}(g)\, T = 1 \oplus \mathsf{U}_{d_2}(g) \oplus \cdots \oplus \mathsf{U}_{d_m}(g) \oplus \cdots \oplus \mathsf{U}_{d_M}(g)\,,$$

where U_{d_m} is a d_m-dimensional irreducible subrepresentation, $\oplus$ denotes the direct sum of matrices, i.e., $A \oplus B = \mathrm{diag}(A, B)$.

The matrix $\mathbb{1}_{\mathsf{N}}$ is the *standard inner product* in any orthonormal basis. In the splitting basis we have the following decomposition of the standard inner product

$$\mathbb{1}_{\mathsf{N}} = \mathbb{1}_{d_1=1} \oplus \cdots \oplus \mathbb{1}_{d_m} \oplus \cdots \oplus \mathbb{1}_{d_M}\,.$$

The *inverse image* of this decomposition in the original permutation basis is

$$\mathbb{1}_{\mathsf{N}} = \mathcal{B}_1 + \cdots + \mathcal{B}_m + \cdots + \mathcal{B}_M,$$

where $\mathcal{B}_m$ is defined by

$$T^{-1}\mathcal{B}_m T = \mathbb{0}_{1+d_2+\cdots+d_{m-1}} \oplus \mathbb{1}_{d_m} \oplus \mathbb{0}_{d_{m+1}+\cdots+d_M}\,.$$

The main idea of the algorithm is based on the fact that $\mathcal{B}_m$'s form a complete set of *orthogonal projectors*, i.e., they are *idempotent*, $\mathcal{B}_m^2 = \mathcal{B}_m$, and mutually *orthogonal*, $\mathcal{B}_m \mathcal{B}_{m'} = \mathbb{0}_{\mathsf{N}}$ if $m \neq m'$. We see that all $\mathcal{B}_m$'s can be obtained as solutions of the *idempotency equation* $X^2 - X = \mathbb{0}_{\mathsf{N}}$ for the generic invariant form $X = x_1\mathcal{A}_1 + \cdots + x_{\mathrm{R}}\mathcal{A}_{\mathrm{R}}$. This is a system of quadratic polynomial equations in the indeterminates $x_1, x_2, \ldots, x_{\mathrm{R}}$. The polynomial system can be computed by using the multiplication table. Let us write the projector in the basis of invariant forms: $\mathcal{B}_m = b_{m,1}\mathcal{A}_1 + b_{m,2}\mathcal{A}_2 + \cdots + b_{m,\mathrm{R}}\mathcal{A}_{\mathrm{R}}$. It is easy to show that $b_{m,1} = d_m/\mathsf{N}$. Thus, any solution of the idempotency system has the form $[x_1^* = d/\mathsf{N}, x_2^*, \ldots, x_{\mathrm{R}}^*]$, where $d \in [1..\mathsf{N}-1]$ is either an irreducible dimension or a sum of such dimensions.

The core part of the algorithm is constructed as follows.

We set initially $E(x_1, x_2, \ldots, x_{\mathrm{R}}) \leftarrow \left\{X^2 - X = \mathbb{0}_{\mathsf{N}}\right\}$.

Then we perform a loop on dimensions that starts with $d = 1$ and ends when the sum of irreducible dimensions becomes equal to N.

For the current d we solve the system of equations $E(d/\mathsf{N}, x_2, \ldots, x_{\mathrm{R}})$. All solutions belong to abelian extensions of $\mathbb{Q}$, so their getting is always algorithmically realizable.

If the system is incompatible, then go to the next d.

If $E(d/\mathsf{N}, x_2, \ldots, x_{\mathrm{R}})$ describes a zero-dimensional ideal, then we have k (including the case $k = 1$) different d-dimensional irreducible subrepresentations.

If the polynomial ideal has dimension $h > 0$, then we encounter an irreducible component with a multiplicity k, where $\lfloor k^2/2 \rfloor = h$. In this case we select, by a somewhat arbitrary procedure, k convenient mutually orthogonal representatives in the family of equivalent subrepresentations.

In any case, if at the moment we have a solution $\mathcal{B}_m$, we append $\mathcal{B}_m$ to the list of irreducible projectors, and exclude from the further consideration the corresponding invariant subspace by adding the linear *orthogonality condition* $\mathcal{B}_m X = \mathbb{0}_{\mathsf{N}}$ to the polynomial system:

$$E(x_1, x_2, \ldots, x_{\mathrm{R}}) \leftarrow E(x_1, x_2, \ldots, x_{\mathrm{R}}) \cup \{\mathcal{B}_m X = \mathbb{0}_{\mathsf{N}}\}.$$

After processing all $\mathcal{B}_m$'s of dimension d, go to the next d.

The complete algorithm is implemented by two procedures:

1. The procedure `PreparePolynomialData` is a program written in **C**. The input data for this program is a set of permutations of Ω that generates the group G. The program computes the basis of the centralizer ring and its multiplication table, constructs the idempotency and orthogonality polynomials, and generates the code of the procedure `SplitRepresentation` that processes the polynomial data. The implementation is able to cope with dimensions (dimension$= |\Omega|$) up to several hundred thousand on a PC within a reasonable time.
2. The procedure `SplitRepresentation` implements the above described loop on dimensions that splits the representation of the group into irreducible components. It is generated by the **C** program `PreparePolynomialData`. Currently, the code is generated in the **Maple** language, and the polynomial equations are processed by the **Maple** implementation of the Gröbner bases algorithms.

Comparison with the **Magma** implementation of the *MeatAxe*.

The **Magma** database contains a 3906-dimensional representation of the exceptional group of Lie type $G_2(5)$. This representation (over the field GF(2)) is used in [4] as an illustration of the capabilities of the *MeatAxe*.

The application of our algorithm to this problem — the calculation showed that the splitting field in this case is $\mathbb{Q}$ — produces the following data.

Rank: 4. Suborbit lengths: $1, 30, 750, 3125$.

$$\underline{\mathbf{3906}} \cong \mathbf{1} \oplus \mathbf{930} \oplus \mathbf{1085} \oplus \mathbf{1890}$$

$$\mathcal{B}_{\mathbf{1}} = \frac{1}{3906}\sum_{k=1}^{4}\mathcal{A}_k$$

$$\mathcal{B}_{\mathbf{930}} = \frac{5}{21}\left(\mathcal{A}_1 + \frac{3}{10}\mathcal{A}_2 + \frac{1}{50}\mathcal{A}_3 - \frac{1}{125}\mathcal{A}_4\right)$$

$$\mathcal{B}_{\mathbf{1085}} = \frac{5}{18}\left(\mathcal{A}_1 - \frac{1}{5}\mathcal{A}_2 + \frac{1}{25}\mathcal{A}_3 - \frac{1}{125}\mathcal{A}_4\right)$$

$$\mathcal{B}_{\mathbf{1890}} = \frac{15}{31}\left(\mathcal{A}_1 - \frac{1}{30}\mathcal{A}_2 - \frac{1}{30}\mathcal{A}_3 + \frac{1}{125}\mathcal{A}_4\right)$$

Time **C**: 1.14 sec. Time **Maple**: 0.8 sec.
The **Magma** fails to split the 3906-dimensional representation over the field $\mathbb{Q}$, but we can model to some extent the case of characteristic zero, using a field of characteristic not dividing $|G_2(5)|$. The smallest such field is GF(11).

Below is the session of the corresponding **Magma** computation on a computer with two Intel Xeon E5410 2.33GHz CPUs (time is given in seconds).

```
> load "g25";
Loading "/opt/magma.21-1/libs/pergps/g25"
The Lie group G( 2, 5 ) represented as a permutation
group of degree 3906.
Order: 5 859 000 000 = 2^6 * 3^3 * 5^6 * 7 * 31.
Group: G
> time Constituents(PermutationModule(G,GF(11)));
[
    GModule of dimension 1 over GF(11),
    GModule of dimension 930 over GF(11),
    GModule of dimension 1085 over GF(11),
    GModule of dimension 1890 over GF(11)
]
Time: 282.060
```

4. Some decompositions for sporadic simple groups.

Generators of representations are taken from the section "Sporadic groups" of the Atlas [6].

Representations are denoted by their dimensions in bold (possibly with some signs added to distinguish different representations of the same dimension).

Permutation representations are underlined.

Multiple subrepresentations are underbraced in the decompositions.

All timing data were obtained on a PC with 3.30GHz Intel Core i3 2120 CPU.

- 1980-dimensional representation of the Mathieu group cover $6.M_{22}$
  Rank: 17. Suborbit lengths: $1^6, 14^3, 84^3, 336^5$.

$$\underline{\mathbf{1980}} \cong \mathbf{1} \oplus \mathbf{21}_\alpha \oplus \mathbf{21}_\beta \oplus \overline{\mathbf{21}_\beta} \oplus \mathbf{55} \oplus \mathbf{99}_\alpha \oplus \mathbf{99}_\beta \oplus \overline{\mathbf{99}_\beta} \oplus \mathbf{105}_+ \oplus \overline{\mathbf{105}_+} \oplus \mathbf{105}_- \oplus \overline{\mathbf{105}_-} \oplus \mathbf{120} \oplus \mathbf{154} \oplus \mathbf{210} \oplus \mathbf{330} \oplus \overline{\mathbf{330}}$$

  Time **C**: 2 sec. Time **Maple**: 8 h 41 min 1 sec.
- 29155-dimensional representation of the Held group *He*
  Rank:12.Suborbit lengths: $1, 90, 120, 384, 960^2, 1440, 2160, 2880^2, 5760, 11520$.

$$\underline{\mathbf{29155}} \cong \mathbf{1} \oplus \mathbf{51} \oplus \overline{\mathbf{51}} \oplus \mathbf{680} \oplus \underbrace{\mathbf{1275} \oplus \mathbf{1275}} \oplus \mathbf{1920} \oplus \mathbf{4352} \oplus \mathbf{7650} \oplus \mathbf{11900}$$

  Time **C**: 5 min 41 sec. Time **Maple**: 15 sec.
- 66825-dimensional representation of the McLaughlin group cover $3.McL$
  Rank: 14. Suborbit lengths: $1^3, 630, 2240^3, 5040^3, 8064^3, 20160$.

$$\underline{\mathbf{66825}} \cong \mathbf{1} \oplus \mathbf{252} \oplus \mathbf{1750} \oplus \mathbf{2772} \oplus \overline{\mathbf{2772}} \oplus \mathbf{5103}_\alpha \oplus \mathbf{5103}_\beta \oplus \overline{\mathbf{5103}_\beta} \oplus \mathbf{5544} \oplus \mathbf{6336} \oplus \overline{\mathbf{6336}} \oplus \mathbf{8064} \oplus \overline{\mathbf{8064}} \oplus \mathbf{9625}$$

  Time **C**: 39 min 36 sec. Time **Maple**: 14 min 11 sec.
- 98280-dimensional representation of the Suzuki group cover $3.Suz$
  Rank: 14. Suborbit lengths: $1^3, 891^3, 2816^3, 5940, 19008, 20736^3$.

$$\underline{\mathbf{98280}} \cong \mathbf{1} \oplus \mathbf{78} \oplus \overline{\mathbf{78}} \oplus \mathbf{143} \oplus \mathbf{364} \oplus \mathbf{1365} \oplus \overline{\mathbf{1365}} \oplus \mathbf{4290} \oplus \overline{\mathbf{4290}} \oplus \mathbf{5940} \oplus \mathbf{12012} \oplus \mathbf{14300} \oplus \mathbf{27027} \oplus \overline{\mathbf{27027}}$$

  Time **C**: 2 h 36 min 29 sec. Time **Maple**: 7 min 41 sec.

References

[1] Holt, D. F., Eick, B., O'Brien, E. A. *Handbook of Computational Group Theory.* Chapman & Hall/CRC, 2005.

[2] Kornyak V. V. Quantum models based on finite groups. *J. Phys.: Conf. Ser.* **965** 012023, 2018. http://stacks.iop.org/1742-6596/965/i=1/a=012023

[3] Kornyak V. V. Modeling Quantum Behavior in the Framework of Permutation Groups. *EPJ Web of Conferences* **173** 01007, 2018. https://doi.org/10.1051/epjconf/201817301007

[4] Bosma, W., Cannon, J., Playoust, C., Steel, A. *Solving Problems with Magma.* University of Sydney. http://magma.maths.usyd.edu.au/magma/pdf/examples.pdf

[5] Cameron P. J. *Permutation Groups.* Cambridge University Press, 1999.

[6] Wilson, R. A., et al., Atlas *of finite group representations.* http://brauer.maths.qmul.ac.uk/Atlas/v3.

Vladimir V. Kornyak
Laboratory of Information Technologies
Joint Institute for Nuclear Research
Dubna, Russia
e-mail: vkornyak@gmail.com

On the Cayley-Bacharach Property

Martin Kreuzer, Le Ngoc Long and Lorenzo Robbiano

Abstract. The Cayley-Bacharach property, which has been classically stated as a property of a finite set of points in an affine or projective space, is extended to arbitrary 0-dimensional affine algebras over arbitrary base fields. We present characterizations and explicit algorithms for checking the Cayley-Bacharach property directly, via the canonical module, and in combination with the property of being a locally Gorenstein ring. Moreover, we characterize strict Gorenstein rings by the Cayley-Bacharach property and the symmetry of their Hilbert function, as well as by the strict Cayley-Bacharach property and the last difference of their Hilbert function.

Extended Abstract

The Cayley-Bacharach Property (CBP) has a long and rich history. Classically, it has been formulated geometrically as follows: *A set of points $\mathbb{X}$ in n-dimensional affine or projective space is said to have the Cayley-Bacharach property of degree d if any hypersurface of degree d which contains all points of $\mathbb{X}$ but one automatically contains the last point.* After a brief recap of its history, we present the currently most general version, namely the definition first given in Ngoc Le Long's Thesis (University of Passau, 2015). Our goal is to study this very general version of the CBP and to find efficient algorithms for checking it. A special emphasis is given to algorithms which will us to apply them to families of 0-dimensional ideals parametrized by border basis schemes. Moreover, we generalize the main results about the CBP of many previous papers to this most general setting of a 0-dimensional affine algebra over an arbitrary base field.

To achieve these goals, we proceed as follows. Our main object of study is a 0-dimensional affine algebra $R = P/I$ over an arbitrary field K, where we let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over K and I a 0-dimensional ideal in P. Even if we do not specify it explicitly everywhere, we always consider R together with this fixed presentation. In other words, we consider a fixed 0-dimensional subscheme $\mathbb{X} = \mathrm{Spec}(P/I)$ of $\mathbb{A}^n$.

This corresponds to the classical setup. However, in the last decades it has been customary to consider 0-dimensional subschemes of projective spaces. Of course, via the standard embedding $\mathbb{A}^n \cong D_+(x_0) \subset \mathbb{P}^n$, the classical setup can be translated to this setting in a straightforward way. For instance, in this case the affine coordinate ring $R = K[x_1, \ldots, x_n]/I$ has to substituted by the homogeneous coordinate ring $R^{\text{hom}} = K[x_0, \ldots, x_n]/I^{\text{hom}}$, etc. In this talk we use the affine setting for several reasons: firstly, the ideals defining subschemes of $\mathbb{X}$ can be studied using the decomposition into local rings, secondly, the structure of the coordinate ring of $\mathbb{X}$ and its canonical module can be described via multiplication matrices, and thirdly, the affine setup is suitable for generalizing everything to families of 0-dimensional ideals via the border basis scheme.

First we recall the primary decomposition $I = \mathfrak{Q}_1 \cap \cdots \cap \mathfrak{Q}_s$ of I, the corresponding primary decomposition $\langle 0 \rangle = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ of the zero ideal of R, and the decomposition $R = R/\mathfrak{q}_1 \times \cdots \times R/\mathfrak{q}_s$ of R into local rings. Then, for $i \in \{1, \ldots, s\}$, a minimal $\mathfrak{Q}_i$-divisor J of I is defined in such a way that the corresponding subscheme of $\mathbb{X}$ differs from $\mathbb{X}$ only at the point $p_i = \mathcal{Z}(\mathfrak{M}_i)$ and has the minimal possible colength $\ell_i = \dim_K(P/\mathfrak{M}_i)$, where $\mathfrak{M}_i = \text{Rad}(\mathfrak{Q}_i)$. In the reduced case, these subschemes are precisely the sets $\mathbb{X} \setminus \{p_i\}$ appearing in the classical formulation of the Cayley-Bacharach Theorem.

Moreover, in order to have a suitable version of degrees, we recall the degree filtration of R, its affine Hilbert function HF^a_R, and its regularity index $\text{ri}(R)$. Here the affine Hilbert function plays the role of the usual Hilbert function if we consider affine algebras such as R.

These constructions are combined with the definition and some characterizations of *separators*. Then we show that a separator for a maximal ideal $\mathfrak{m}_i$ of R corresponds to a generator of a minimal $\mathfrak{Q}_i$-divisor J of I, and we use the maximal order of such a separator to describe the regularity index of J/I. Then the minimum of all regularity indices $\text{ri}(J/I)$ is called the *separator degree* of $\mathfrak{m}_i$. We go on to show that this "minimum of all maxima" definition is the correct, but rather subtle generalization of the classical notion of the least degree of a hypersurface containing all points of $\mathbb{X}$ but p_i.

The separator degree of a maximal ideal $\mathfrak{m}_i$ of R is bounded by the regularity index $\text{ri}(R)$, since the order of any separator is bounded by this number. If all separator degrees attain this maximum value, we say that R has the *Cayley-Bacharach property (CBP)*, or that $\mathbb{X}$ is a *Cayley-Bacharach scheme*. At this point we construct our first new algorithm which allows us to check whether a given maximal ideal $\mathfrak{m}_i$ of R has maximal separator degree.

Although this algorithm can be used to check the CBP of R, we then construct a better one based on the canonical module $\omega_R = \text{Hom}_K(R, K)$ of R. The module structure of ω_R is given by $(f\,\varphi)(g) = \varphi(fg)$ for all $f, g \in R$ and all $\varphi \in \omega_R$. It carries a degree filtration $\mathcal{G} = (G_i\omega_R)_{i\in\mathbb{Z}}$ which is given by $G_i\omega_R = \{\varphi \in \omega_R \mid \varphi(F_{-i-1}R) = 0\}$ and its affine Hilbert function which satisfies $\text{HF}^a_{\omega_R}(i) = \dim_K(R) - \text{HF}^a_R(-i-1)$ for $i \in \mathbb{Z}$. Generalizing some earlier results, we show that the module structure of ω_R is connected to the CBP of R. More precisely, one

main theorem says that R has the CBP if and only if $\mathrm{Ann}_R(G_{-\mathrm{ri}(R)}\omega_R) = \{0\}$. Based on this characterization and the description of the structure of R and the module structure of ω_R via multiplication matrices, we obtain the second main algorithm for checking the CBP of R using the canonical module. As a nice and useful by-product, we show that, for an extension field L of K, the ring R has the CBP if and only if $R \otimes_K L$ has the CBP.

Next we turn our attention to 0-dimensional affine algebras R which are locally Gorenstein and have the CBP. We show that R is locally Gorenstein if and only if ω_R contains an element φ such that $\mathrm{Ann}_R(\varphi) = \{0\}$ and that we can check this effectively. Then we characterize locally Gorenstein rings having the CBP by the existence of an element $\varphi \in \omega_{R\otimes L}$ of order $-\mathrm{ri}(R)$ with $\mathrm{Ann}_{R\otimes L}(\varphi) = \{0\}$. Here we may have to use a base field extension $K \subseteq L$ or assume that K is infinite. This characterization implies useful inequalities for the affine Hilbert function of R and allows us to formulate an algorithm which checks whether R is a locally Gorenstein ring having the CBP using the multiplication matrices of R. To end this discussion, we characterize the CBP of R in the case when the last difference $\Delta_R = \mathrm{HF}_R(\mathrm{ri}(R)) - \mathrm{HF}_R(\mathrm{ri}(R) - 1)$ is one.

The subsequent topic is to characterize 0-dimensional affine algebras which are strict Gorenstein rings. This property means that the graded ring $\mathrm{gr}_{\mathcal{F}}(R)$ with respect to the degree filtration is a Gorenstein ring. In the projective case, the corresponding 0-dimensional schemes are commonly called arithmetically Gorenstein. Our first characterization of strict Gorenstein rings improves earlier results by Davis, Geramita, and Orecchia. More precisely, we show that R is strictly Gorenstein if and only if it has the CBP and a symmetric Hilbert function. In particular, it follows that these rings are locally Gorenstein. Then we define the strict CBP of R by the CBP of $\mathrm{gr}_{\mathcal{F}}(R)$ and show that it implies the CBP of R. Thus we obtain a second characterization of strict Gorenstein rings: R is a strict Gorenstein ring if and only if R has the strict CBP and $\Delta_R = 1$.

In the last part of the talk, we show how one can extend all these characterizations to families of 0-dimensional polynomial ideals. More precisely, we introduce the border basis scheme and explain some ways of getting explicit polynomial equations defining subschemes corresponding to all ideals with a particular property, for instance the CBP.

Martin Kreuzer
Fakultät für Informatik und Mathematik, Universität Passau, D-94030 Passau, Germany
e-mail: Martin.Kreuzer@uni-passau.de

Le Ngoc Long
Fakultät für Informatik und Mathematik, Universität Passau, D-94030 Passau, Germany
e-mail: nglong16633@gmail.com

Lorenzo Robbiano
Dipartimento di Matematica, Università di Genova, Via Dodecaneso 35, I-16146 Genova, Italy
e-mail: lorobbiano@gmail.com

Elliptic functions and finite difference method

Mikhail D. Malykh, Leonid A. Sevastianov and Yu Ying (余英)

Abstract. For some autonomous dynamic systems, especially for equations related to pendulum oscillation and top rotation, new finite difference schemes are suggested.

Standard considerations of integrability of differential equations in symbolic form refer to the computational techniques of the past centuries. For example, in the studies of Galois differential theory, they use the concept of elementary functions. In the times of Liouville, when these studies were initiated, the functions have been considered elementary if their tables were available for common use. At present, this class of functions is much narrower than the set of functions, for which the computation algorithms are implemented in all systems of computer algebra.

Among different approaches to the concept of integrability in the symbolic form a special position is occupied by the approach proposed in the first papers by Painlevé and then forgotten for long [1]. The idea is that in most cases, when the differential equation

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

is integrated in a finite form, the general solution depends on the integration constants algebraically, even when the dependence upon x is described by rather complicated transcendental functions. This property is purely algebraic, which makes it possible to construct an analogue of the Galois theory, where the class of admissible transcendental operations is described in the course of the theory development, rather than being fixed as in the Liouville approach. The approach yields all classical transcendental function, from cylindrical to Abelian ones [2, 3].

There is a rather nontrivial connection between this version of Galois theory, and the finite difference method. If the general solution of the differential equation

$$y' = f(x, y), \quad f \in \mathbb{Q}(x, y),$$

depends on the constant algebraically, then it can be approximated by a difference scheme, defining the projective correspondence between the layers. The main difference of this scheme from the commonly used ones is that it allows one to

continue the calculation beyond the movable singular points without considerable accumulation of error [4].

A natural assumption is that for other classes of sets of differential equations, for which the general solution depends on the constants algebraically, one can construct difference schemes that allows one to continue the computations over wider intervals. In other words, the classical transcendental functions are particular solutions of such differential equations, for which the solution using the finite difference method is particularly efficient. In the present report, we would like to consider one of the most important class of such functions, namely, the elliptic functions.

The elliptic functions appeared in mechanics as higher transcendental functions that provide the integration of various problems related to pendulum oscillation and top rotation. In these cases, the equations of motion can be considered as particular cases of the autonomous dynamic system

$$\dot{\vec{x}} = f(\vec{x}),$$

possessing a few integrals of motion. Standard explicit difference schemes do not conserve these integrals; therefore, their use for calculations over the time of about ten periods yields an approximate solution that is considerably aperiodic. For a top with the fixed center of gravity, the integrals of motion are quadratic, so they are conserved by the symplectic Runge-Kutta schemes [5]. However, in the present case all these schemes will be implicit. For example, the transition from one layer to another in the single-stage scheme will require the solution of a fifth-power equation, which essentially complicates practical application of such schemes.

Problem. Given a system of differential equations and a few integrals, construct an explicit difference scheme, exactly conserving the integrals of motion.

In the present report we restrict ourselves to the case, when the integrals of motion specify a curve of the genus ρ in the space, where $\vec{x}$ varies. In this case, any difference scheme is an algebraic transformation of this curve. Therefore, at $\rho > 1$ the desired difference scheme does not exist for purely geometric reasons (Zeuthen-Hurwitz theorems). At $\rho = 1$ (elliptic curve) the explicit formulae for birational transformations are known, so that it is always possible to check, whether these formulae approximate the given differential equation or not. In the case of a top, the answer is positive, and an explicit difference scheme for the approximate solutions can be constructed. Without any relation to the theory of difference schemes, this method of calculating the elliptic functions has been applied to the composition of the first tables by Ch. Gudermann [6]. In the report, we consider the properties of this scheme.

We believe that all transcendental functions can be reconsidered as solutions of such differential equations, for which the application of the finite difference method is particularly efficient.

References

[1] *Umemura H.* Nagoya Math. J. 1990. Vol. 119, pp. 1–80.
[2] *Malykh M.D.* Journal of Mathematical Sciences. 2015. Vol. 209. No. 6, pp. 935–952.
[3] *Malykh M.D.* Polynomial Computer Algebra '2014, pp. 52–53.
[4] *Malykh M.D.* Polynomial Computer Algebra '2015, pp. 57–58.
[5] *Sanz-Serna J.M.* SIAM Review. 2016. Vol. 58, No. 1, pp. 3–33.
[6] *Weierstrass K.* Bb. 1. Abh. 1. Berlin: Mayer&Müller, 1894.

Mikhail D. Malykh
Department of Applied Probability and Informatics
Peoples' Friendship University of Russia,
Moscow, Russia

e-mail: malykhmd@yandex.ru

Leonid A. Sevastianov
Department of Applied Probability and Informatics
Peoples' Friendship University of Russia,
Moscow, Russia

e-mail: leonid.sevast@gmail.com

Yu Ying (余英)
Department of Applied Probability and Informatics
Peoples' Friendship University of Russia,
Moscow, Russia

e-mail: yuying05720062@sina.com

What does a random knot look like?

Andrei Malyutin

Abstract. We discuss the structure and statistics of the set of classical knots and present new results in this research area.

We study the structure and statistical characteristics of the set of classical knots. Closely related topics are statistics of links, tangles, 3-manifolds, graph embeddings, plane diagrams, meanders, countable groups, elements of mapping class groups, braids, etc. The question we primarily address is what does a typical large (prime) knot look like. Probabilistic wording for this question is as follows: what properties does a random (prime) knot have?

What properties of knots does it make sense to check for genericity? Nice candidates come from the basic knot classification. The first level of the classification splits the set of non-trivial knots into the subclasses of prime and composite ones. The second level divides prime knots into the satellite (with incompressible tori in the complement) and simple ones. Similar classifications hold for links, 3-manifolds, etc. Thurston proved that the complement of every simple knot bears a geometric structure: every simple knot is either torus or hyperbolic. This yields the following tree of knots basic properties:

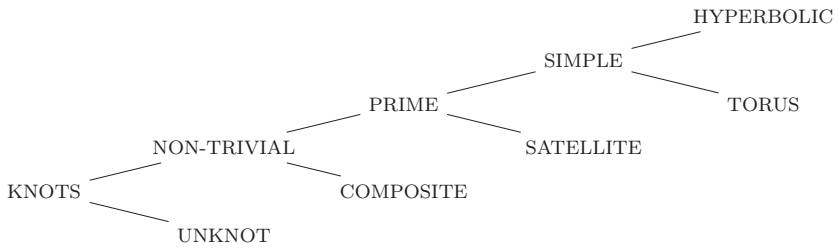


FIGURE 1. The tree of basic knot classes.

Supported by RFBR grant 16-01-00609.

The dual question to the previous one is which random knot model we choose. Dozens of such models are described in the literature (see [4]). We discuss several of them that are either natural, well-studied, or have specific properties that are of particular interest to our discussion. Our list includes the following:

- random walk models (a random knot is a random polygon in $\mathbb{R}^3$ whose edge vectors are guided by some non-degenerate probability distribution);
- braid group models (we consider knots and links that are Alexander/plat closures of randomly generated braids);
- knot tables model (we consider uniform measures on the sets of knots with crossing number at most n);
- random jump model (a random knot is a random polygon in $\mathbb{R}^3$ whose vertices are guided by the same non-degenerate probability distribution).

An interesting issue related to the above properties of knots is the balance between hyperbolic knots and satellites. For a rather long period of time it was widely believed that most knots and links are hyperbolic (see, e. g., [12, p. 507]). The reason is that the sets of torus and satellite knots look rather special and rare and give an impression of scarcity. In particular, only 32 of the first 1 701 936 prime knots are non-hyperbolic (see [5]). Another related fact is that hyperbolic knots are generic in the braid group models (see [9, 7, 6]).

However, a deeper analysis shows that the conjecture of the hyperbolic knots prevalence is quite flimsy. Indeed, the braid group models are highly imbalanced, and the case with 1 701 936 knots can be explained by the fact that satellites are relatively large, which does not imply asymptotic scarcity. Furthermore, there is (indirect) evidence that the satellites persist in random walk models (see [8, 3]). In addition, the conjecture that hyperbolic knots are asymptotically generic in prime knot tables (see [1]) contradicts several other plausible conjectures (see [10, 11]). This is due to the fact that satellite structures should be large enough, but they can be local (see [11]). We also present the following new evidence related to the tables model.

Theorem 1. *The percentage of hyperbolic links amongst all of the prime non-split links of n or fewer crossings does not tend to* 100 *as n tends to infinity.*

In models where a random knot is satellite, it is interesting to study its companionship tree (see [2]).

It would seem that the above arguments indicate satellite knots predominance. However, we conjecture that the space of knots is complex enough to have several natural well-balanced random knot models showing opposite behavior. In this regard, we present the following new conjecture related to the random jump model.

Conjecture 1. *Hyperbolic knots are generic in the random jump model.*

Expected behavior of distinct random knot models is presented in Table 1.

model \ set of knots	all knots	prime knots
random walk models	composite (proved)	satellite (str. conj.)
braid group models	hyperbolic (proved)	hyperbolic (proved)
knot tables model	composite (str. conj.)	satellite (str. conj.)
random jump model	hyperbolic (weak conj.)	hyperbolic (weak conj.)

TABLE 1. Generic types of knots in several models.

References

[1] C. C. Adams, *The Knot Book: An Elementary Introduction to the Mathematical Theory of Knots*, New York, W. H. Freeman and Company, 1994.

[2] R. Budney, *JSJ-decompositions of knot and link complements in S^3*, Enseign. Math. (2) **52**:2 (2006), 319–359.

[3] Y. Diao, J. C. Nardo, and Y. Sun, *Global knotting in equilateral random polygons*, J. Knot Theory Ramifications **10**:4 (2001), 597–607.

[4] C. Even-Zohar, *Models of random knots*, J. Appl. Comput. Topology **1**:2 (2017), 263–296.

[5] J. Hoste, M. Thistlethwaite, and J. Weeks, *The first 1,701,936 knots*, Math. Intelligencer **20**:4 (1998), 33–48.

[6] K. Ichihara and J. Ma, *A random link via bridge position is hyperbolic*, Topology Appl. **230** (2017), 131–138.

[7] T. Ito, *On a structure of random open books and closed braids*, Proc. Japan Acad. Ser. A Math. Sci. **91**:10 (2015), 160–162.

[8] D. Jungreis, *Gaussian random polygons are globally knotted*, J. Knot Theory Ramifications **3**:4 (1994), 455–464.

[9] J. Ma, *The closure of a random braid is a hyperbolic link*, Proc. Amer. Math. Soc. **142**:2 (2014), 695–701.

[10] A. V. Malyutin, *Satellite knots strike back*, Abstracts of the International Conference "Polynomial Computer Algebra '15" (2015), 65–66.

[11] A. V. Malyutin, *On the question of genericity of hyperbolic knots*, preprint (2016), arXiv:1612.03368.

[12] J. G. Ratcliffe, *Foundations of Hyperbolic Manifolds*, Grad. Texts in Math. 149, Springer, New York, 2nd edition, 2006.

Andrei Malyutin
St. Petersburg Department of
Steklov Institute of Mathematics
St. Petersburg State University
St. Petersburg, Russia
e-mail: malyutin@pdmi.ras.ru

On Strongly Consistent Finite Difference Approximations

Dominik Michels, Vladimir Gerdt, Dmitry Lyakhov and Yuri Blinkov

Solving partial differential equations (PDEs) belongs to the most fundamental and practically important research challenges in mathematics and in the computational sciences. Such equations are typically solved numerically since obtaining their explicit solution is usually very difficult in practice or even impossible. One of the classical and nowadays well-established and popular approaches is the finite difference method [1, 2, 3] which exploits a local Taylor expansion to replace a differential equation by the difference one. This raises the question how to preserve fundamental properties of the underlying PDEs at the discrete level. From a geometric point of view, the most important properties are symmetries and conservation laws. Importance of conservation laws in mathematical physics could not be underestimated, since many fundamental properties for nonlinear PDEs (like existence and uniqueness of solutions) typically are based on conservation laws. From algebraic perspective, the basic object which should be preserved is algebraic relations between equations and their differential (difference) consequences. The problem here occurs because finite difference approximation of derivation doesn't satisfy Leibnitz rule.

The fundamental requirement of a finite difference scheme (FDS) is its convergence to a solution of the corresponding differential problem as the grid spacings go to zero. According to the Lax-Richtmyer equivalence theorem [4, 5], for a scalar PDE it has been adopted that the convergence is provided if a given finite-difference approximation (FDA) to the PDE is consistent and stable. The consistency implies a reduction of the FDA to the original PDE when the grid spacings go to zero, and it is obvious that the consistency is necessary for convergence. The theorem states that a FDS for an initial value (Cauchy) problem providing the existence and uniqueness of the solution converges if and only if its FDA is consistent and numerically stable.

In this talk we describe algorithmic methods to generate FDAs to PDEs on orthogonal and uniform grids, and to verify strong consistency of the obtained FDAs. The main algorithmic tool for the case of linear PDEs is the difference elimination provided by Groebner bases [6, 7, 8] for a certain elimination ranking.

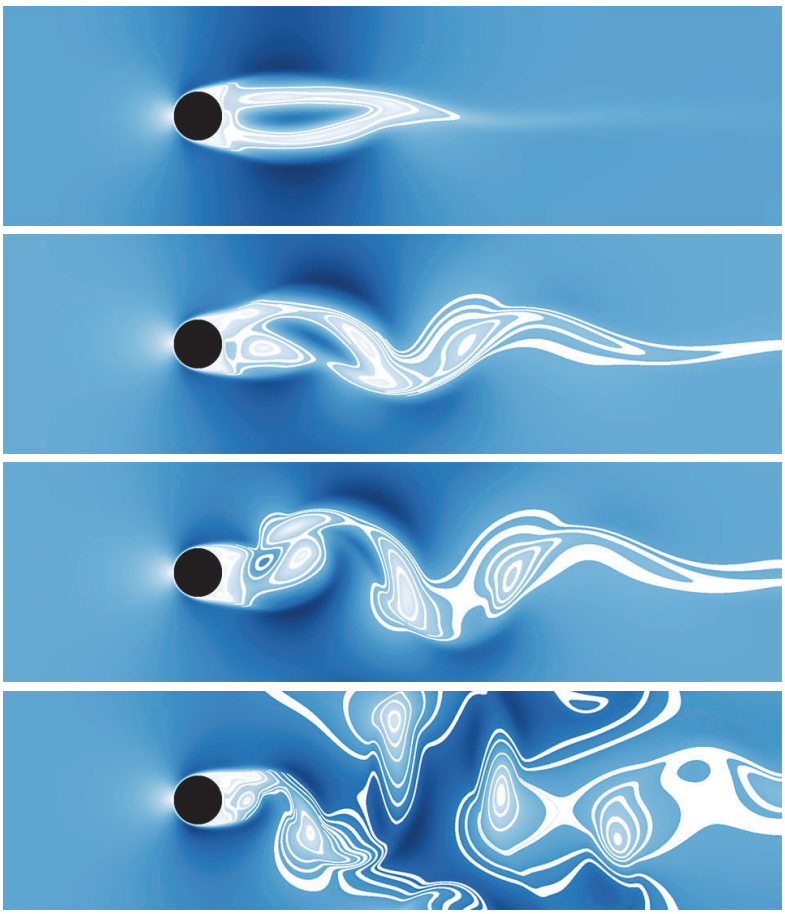


FIGURE 1. Simulation of the Kármán vortex street computed with the new FDA. The characteristic repeating pattern of swirling vortices can be observed, cf. [15].

Given a system of polynomially-nonlinear PDEs and its FDA, the s-consistency analysis is based on a computation of a difference standard Groebner basis and the construction of a differential Thomas decomposition [9, 10] for the PDE system. This talk is an extension of the methodology of [8, 11, 12, 13, 14]. As a relevant example in practice, we apply the procedure of the strong consistent FDA generation to the two-dimensional Navier-Stokes equations for the unsteady motion of an incompressible fluid of constant viscosity. For these equations, we construct

two fully conservative FDAs (one s-consistent and one w-consistent). We use the FDAs for the numerical simulation on exact solutions and consider a Kármán vortex street to analyze the influence of the consistency on the numerical quality of these schemes.

References

[1] Godunov, S.K., Ryaben'kii, V.S.: Difference schemes. An introduction to the underlying theory. Elsevier, New York (1987).

[2] Morton, K.W., Mayers, D.F.: Numerical Solution of Partial Differential Equations. An Introduction, Cambridge University Press, (2005).

[3] Samarskii, A.A.: Theory of Difference Schemes. Marcel Dekker, New York (2001).

[4] Strikwerda, J.C.: Finite Difference Schemes and Partial Differential Equations, 2nd Edition. SIAM, Philadelphia (2004).

[5] Thomas, J.W.: Numerical Partial Differential Equations: Finite Difference Methods, 2nd Edition. Springer, New York (1998).

[6] Gerdt, V.P., Robertz, D.: Computation of Difference Groebner Bases. Comp. Sci. J. of Moldova 20, No.2(59), 203–226 (2012).

[7] Levin, A.: Difference Algebra. Algebra and Applications, Vol. 8. Springer (2008).

[8] Gerdt, V.P.: Consistency Analysis of Finite Difference Approximations to PDE Systems. Mathematical Modelling in Computational Physics / MMCP 2011, Adam, G., Buša, J., Hnatič, M. (Eds.), LNCS 7125, pp. 28–42. Springer, Berlin (2012). arXiv:math.AP/1107.4269

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

[10] Robertz, D.: Formal Algorithmic Elimination for PDEs. Lecture Notes in Mathematics 2121. Springer, Cham (2014).

[11] Amodio, P., Blinkov Yu.A., Gerdt, V.P. and La Scala, R.: Algebraic construction and numerical behavior of a new s-consistent difference scheme for the 2D Navier–Stokes equations. Applied Mathematics and Computation, 314, pp.408-421. (2017).

[12] Gerdt, V.P., Blinkov, Yu.A., Mozzhilkin, V.V.: Groebner Bases and Generation of Difference Schemes for Partial Differential Equations. SIGMA 2, 051 (2006). arXiv:math.RA/0605334

[13] Gerdt, V.P., Blinkov, Yu.A.: Involution and Difference Schemes for the Navier-Stokes Equations. Computer Algebra in Scientific Computing / CASC 2009, Gerdt, V.P., Mayr, E.W., Vorozhtsov, E.V. (Eds.), LNCS 5743, pp. 94–105. Springer, Berlin (2009).

[14] Gerdt, V.P., Robertz, D.: Consistency of Finite Difference Approximations for Linear PDE Systems and its Algorithmic Verification. Watt, S.M. (Ed.), Proceedings of ISSAC 2010, pp. 53–59. Association for Computing Machinery (2010).

[15] Kármán, T.: Aerodynamics. McGraw-Hill, New York (1963).

Dominik Michels
Visual Computing Center
King Abdullah University of Science and Technology
Thuwal, Saudi Arabia
e-mail: dominik.michels@kaust.edu.sa

Vladimir Gerdt
Laboratory of Information Technologies
Joint Institute for Nuclear Research
Dubna, Russia
e-mail: gerdt@jinr.ru

Dmitry Lyakhov
Visual Computing Center
King Abdullah University of Science and Technology
Thuwal, Saudi Arabia
e-mail: dmitry.lyakhov@kaust.edu.sa

Yuri Blinkov
Faculty of Mechanics and Mathematics
Saratov State University
Saratov, Russian Federation
e-mail: blinkovua@info.sgu.ru

On finite subgroups of SO(3), regular polyhedrons in R4 and the spherical motion of rigid body

Evgenii A. Mityushov, Natalia E. Misyura and Svetlana A. Berestova

Based on the fact of two-sheeted covering group SO(3) by group of unit quarternions Sp(1) and vertices coordinates of tesseract, 16-cell, 24-cell, 120-cell, 600-cell, their images are found in the way of equal distribution of dots on the unit sphere S3. Animation of smooth spherical motion of rigid body along the shortest [1] and random [2] path through the nodes of the resulting graph for 24-cells is done by the method of nonlinear interpolation of quarternions. Spherical motion of rigid body is associated with the movement of the point on the hypersphere in four-dimensional space along the arcs of large circle through the vertices of regular four-dimensional polytope. For an analytical presentation of the law of continuous movement used the original algebraic representation of the Heaviside function. The algorithm allows in a wide range to change the time intervals displacements between nodes, as well as the laws of motion on these intervals. Many tasks of motion control and navigation, robotics and computer graphics relate with the description of a rigid body rotation in three-dimensional space. We give a constructive solution for the smooth movement of a rigid body to solve such problems [3, 4].

References

[1] `https://www.youtube.com/watch?v=_k00jJIBqWY`.

[2] `https://www.youtube.com/watch?v=KwqQVov83jk`.

[3] S.A. Berestova, N.P. Kopytov, E.A. Mityushov, *Engineering Journal: Science and Innovation*, 7, 2017.

[4] E.A. Mityushov, N.E. Misyura, S.A. Berestova, *The Bulletin of Udmurt University. Mathematics. Mechanics. Computer Science*, 27, 1, 2017.

Evgenii A. Mityushov
Department of theoretical mechanics
Ural Federal University named after the first President of Russia B.N.Yeltsin
Ekaterinburg, Russia
e-mail: mityushov-e@mail.ru

Natalia E. Misyura
Department of theoretical mechanics
Ural Federal University named after the first President of Russia B.N.Yeltsin
Ekaterinburg, Russia
e-mail: n.e.misiura@urfu.ru

Svetlana A. Berestova
Department of theoretical mechanics
Ural Federal University named after the first President of Russia B.N.Yeltsin
Ekaterinburg, Russia
e-mail: s.a.berestova@urfu.ru

On the chordality of polynomial sets in triangular decomposition in top-down style

Chenqi Mou

Abstract. In this talk, we show the connections between chordal graphs which permit perfect elimination orderings on their vertexes from Graph Theory and triangular decomposition which decompose polynomial sets into triangular sets from Computer Algebra and present the chordal graph structures of polynomial sets appearing in triangular decomposition in top-down style when the input polynomial set has a chordal associated graph. In particular, we show that the associated graph of one specific triangular set in any algorithm for triangular decomposition in top-down style is a subgraph of that chordal graph and that all the triangular sets computed by Wang's method for triangular decomposition have associated graphs which are subgraphs of that chordal graph. Furthermore, the associated graphs of polynomial sets can be used to describe their sparsity with respect to the variables, and we present a refined algorithm for efficient triangular decomposition for sparse polynomial sets in this sense.

This talk is based on the joint work with Yang Bai.

1. Chordal graphs and triangular decomposition

Let $\mathbb{K}$ be a field, and $\mathbb{K}[\boldsymbol{x}]$ be the multivariate polynomial ring over $\mathbb{K}$ in the variables $x_1, \ldots, x_n$.

For a polynomial $F \in \mathbb{K}[\boldsymbol{x}]$, define the (variable) *support* of F, denoted by $\mathrm{supp}(F)$, to be the set of variables in $x_1, \ldots, x_n$ which effectively appear in F. For a polynomial set $\mathcal{F} \subset \mathbb{K}[\boldsymbol{x}]$, $\mathrm{supp}(\mathcal{F}) := \cup_{F \in \mathcal{F}} \mathrm{supp}(F)$, and its *associated graph* $G(\mathcal{F}) = (V, E)$ is an undirected graph with $V = \mathrm{supp}(\mathcal{F})$ and $E = \{(x_i, x_j) : \exists F \in \mathcal{F}$ such that $x_i, x_j \in \mathrm{supp}(F)\}$.

Let $G = (V, E)$ be a graph with $V = \{x_1, \ldots, x_n\}$. Then an ordering $x_{i_1} < x_{i_2} < \cdots < x_{i_n}$ of the vertexes is called a *perfect elimination ordering* of G if for each $j = i_1, \ldots, i_n$, the restriction of G on the set $\{x_j\} \cup \{x_k : x_k < x_j$ and $(x_k, x_j) \in E\}$ is a clique. A graph G is said to be *chordal* if there exists a perfect elimination ordering of it and a polynomial set $\mathcal{F} \subset \mathbb{K}[\boldsymbol{x}]$ is said to be *chordal* if $G(\mathcal{F})$ is chordal.

For example, the associated graph of $\mathcal{P} = \{x_2 + x_1, x_3 + x_1, x_4^2 + x_2, x_4^3 + x_3, x_5 + x_2, x_5 + x_3 + x_2\}$ is shown in Figure 1. One can find that the associated graph $G(\mathcal{P})$ is chordal by definition and thus $\mathcal{P}$ is chordal.

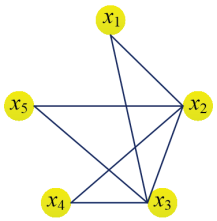


FIGURE 1. The associated graphs $G(\mathcal{P})$

Let the variables in $\mathbb{K}[\boldsymbol{x}]$ be ordered as $x_1 < \cdots < x_n$. An ordered set of non-constant polynomials $\mathcal{T} \subset \mathbb{K}[\boldsymbol{x}]$ is called a *triangular set* if the greatest variables of the polynomials in $\mathcal{T}$ increase strictly. A finite number of triangular sets $\mathcal{T}_1, \ldots, \mathcal{T}_r \subset \mathbb{K}[\boldsymbol{x}]$ are called a *triangular decomposition* of a polynomial set $\mathcal{F} \subset \mathbb{K}[\boldsymbol{x}]$ if $\mathsf{Z}(\mathcal{F}) = \cup_{i=1}^{r} (\mathsf{Z}(\mathcal{T}_i) \setminus \mathsf{Z}(\prod_{T \in \mathcal{T}_i} \mathrm{ini}(T))$ holds, where $\mathrm{ini}(T)$ is the leading coefficient of T with respect to the greatest variable of T and $\mathsf{Z}(\cdot)$ denotes the set of common zeros.

Roughly speaking, an algorithm $\mathcal{A}$ for computing triangular decomposition of $\mathcal{F} \subset \mathbb{K}[\boldsymbol{x}]$ is said to be in *top-down style* if the elimination of variables in $\mathcal{A}$ follows a strict order $x_n, x_{n-1}, \ldots, x_1$ and in the process of eliminating each x_i $(1 \leq i \leq n)$, no variables greater than x_i (namely $x_{i+1}, \ldots, x_n$) are generated.

2. Main theoretical results

2.1. General algorithms for triangular decomposition in top-down style

Denote the power set of a set S by 2^S. For an integer i $(1 \leq i \leq n)$, let f_i be a mapping

$$\begin{aligned} f_i : 2^{\mathbb{K}[\boldsymbol{x}_i] \setminus \mathbb{K}[\boldsymbol{x}_{i-1}]} &\to (\mathbb{K}[\boldsymbol{x}_i] \setminus \mathbb{K}[\boldsymbol{x}_{i-1}]) \times 2^{\mathbb{K}[\boldsymbol{x}_{i-1}]} \\ \mathcal{P} &\mapsto (T, \mathcal{R}) \end{aligned} \tag{1}$$

such that $\mathrm{supp}(T) \subset \mathrm{supp}(\mathcal{P})$ and $\mathrm{supp}(\mathcal{R}) \subset \mathrm{supp}(\mathcal{P})$. For a polynomial set $\mathcal{P} \subset \mathbb{K}[\boldsymbol{x}]$ and a fixed integer i $(1 \leq i \leq n)$, suppose that $(T_i, \mathcal{R}_i) = f_i(\mathcal{P}^{(i)})$ for some f_i as stated above. For $j = 1, \ldots, n$, define the polynomial set

$$\mathrm{red}_i(\mathcal{P}^{(j)}) := \begin{cases} \mathcal{P}^{(j)}, & \text{if } j > i \\ \{T_i\}, & \text{if } j = i \\ \mathcal{P}^{(j)} \cup \mathcal{R}_i^{(j)}, & \text{if } j < i \end{cases}$$

and $\mathrm{red}_i(\mathcal{P}) := \cup_{j=1}^{n} \mathrm{red}_i(\mathcal{P}^{(j)})$. In particular, write

$$\overline{\mathrm{red}}_i(\mathcal{P}) := \mathrm{red}_i(\mathrm{red}_{i+1}(\cdots(\mathrm{red}_n(\mathcal{P}))\cdots)) \tag{2}$$

for simplicity.

The mapping f_i in (1) is abstraction of specific reductions with respect to one variable x_i used in different kinds of algorithms for triangular decomposition in top-down style.

Theorem 2.1. *Let $\mathcal{F} \subset \mathbb{K}[\boldsymbol{x}]$ be a chordal polynomial set with $x_1 < \cdots < x_n$ as one perfect elimination ordering and $\overline{\mathrm{red}}_i(\mathcal{F})$ be defined in* (2) *for $i = n, \ldots, 1$. Then the following statements hold:*

(a) *For each $i = n, \ldots, 1$, $G(\overline{\mathrm{red}}_i(\mathcal{F})) \subset G(\mathcal{F})$.*
(b) *If $\mathcal{T} := \overline{\mathrm{red}}_1(\mathcal{F})$ does not contain any nonzero constant, then $\mathcal{T}$ forms a triangular set such that $G(\mathcal{T}) \subset G(\mathcal{F})$.*

Theorem 2.1 (b) tells us that under the conditions stated in the theorem, the associated graph of one specific triangular set computed in any algorithm for triangular decomposition in top-down style is a subgraph of the associated graph of the input polynomial set. In fact, this triangular set is the "main branch" in the triangular decomposition in the sense that other branches are obtained by adding additional constrains in the splitting in the process of triangular decomposition.

2.2. Wang's method for triangular decomposition

A simply-structured algorithm was proposed by Wang for triangular decomposition in top-down style in 1993 [2]. The decomposition process in Wang's method applied to a polynomial set $\mathcal{F} \subset \mathbb{K}[\boldsymbol{x}]$ can be viewed as a binary tree with its root as $(\mathcal{F}, \emptyset, n)$.

Theorem 2.2. *Let $\mathcal{F} \subset \mathbb{K}[\boldsymbol{x}]$ be a chordal polynomial set with $x_1 < \cdots < x_n$ as one perfect elimination ordering and $(\mathcal{P}, \mathcal{Q}, i)$ be any node in the binary decomposition tree for Wang's method applied to $\mathcal{F}$. Then $G(\mathcal{P}) \subset G(\mathcal{F})$. In particular, let $\mathcal{T}_1, \ldots, \mathcal{T}_r$ be the triangular sets computed by Wang's method. Then $G(\mathcal{T}_i) \subset G(\mathcal{F})$ for $i = 1, \ldots, r$.*

As shown by Theorem 2.2, with a chordal input polynomial set, all the polynomials in the nodes of the decomposition tree of Wang's method, and thus all the computed triangular sets, have associated graphs which are subgraphs of that of the input polynomial set.

3. Fast triangular decomposition for variable sparse polynomial sets

Let $G(\mathcal{F}) = (V, E)$ be the associated graph of a polynomial set $\mathcal{F} \subset \mathbb{K}[\boldsymbol{x}]$. Then the *variable sparsity* $s_v(\mathcal{F})$ of $\mathcal{F}$ can be defined as

$$s_v(\mathcal{F}) = |E| / \binom{2}{|V|},$$

where the denominator is the number of edges of a complete graph composed of $|V|$ vertexes. Triangular decomposition of a chordal and variable sparse polynomial set $\mathcal{F} \subset \mathbb{K}[\boldsymbol{x}]$ with an algorithm in top-down style can be sped up by using the perfect elimination ordering of the chordal associated graph $G(\mathcal{F})$.

Some experimental comparisons of timings for computing regular decomposition of one class of chordal and variable sparse polynomials [1]

$$\mathcal{F}_i := \{x_k x_{k+3} - x_{k+1}x_{k+2} : k = 1, 2, \ldots, i\ \}, \quad i \in \mathbb{Z}_{>0}$$

with respect to the perfect elimination ordering versus random orderings are reported in the following table, where n denotes the variable number in $\mathcal{F}_i$, s_v denotes the variable sparsity, t_p and t_r are the timings (in seconds) for regular decomposition with respect to the perfect elimination orderings and 5 randomly chosen variable orderings respectively, and $\bar{t}_r$ are the average timings for random orderings.

TABLE 1. Timings for regular decomposition of $\mathcal{F}_i$

n	s_v	t_p	t_r					$\bar{t}_r$	$\bar{t}_r/t_p$
8	0.64	0.11	0.10	0.09	0.05	0.06	0.09	0.10	0.91
10	0.53	0.19	0.14	0.21	0.22	0.11	0.21	0.18	0.95
20	0.28	1.44	4.24	4.45	3.15	4.41	4.65	4.18	2.90
25	0.23	4.25	50.62	20.29	15.55	25.01	35.10	29.31	6.90
30	0.19	11.94	177.37	185.94	130.54	142.97	103.42	148.05	12.40
35	0.17	42.33	560.56	291.35	633.43	320.98	938.45	548.95	12.97
40	0.15	161.11	1883.64	3618.04	4289.13	4013.99	2996.37	3360.23	20.86

References

[1] Diego Cifuentes and Pablo A Parrilo. Chordal networks of polynomial ideals. *SIAM J. Appl. Algebra Geom.*, 1(1):73–110, 2017.

[2] Dongming Wang. An elimination method for polynomial systems. *J. Symbolic Comput.*, 16(2):83–114, 1993.

Chenqi Mou
LMIB – School of Mathematics and Systems Science
Beijing Advanced Innovation Center for Big Data and Brain Computing
Beihang University, Beijing 100191, China
e-mail: chenqi.mou@buaa.edu.cn

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

Mylläri Aleksandr, Mylläri Tatiana, Myullyari Anna and Vassiliev Nikolay

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

We analyse complexity of trajectories in the equal-mass free-fall three-body problem by numerically constructing symbolic sequences and calculating different entropy-like parameters for these sequences. We also discuss some ways to estimate Kolmogorov and Kolmogorov-Sinai entropy.

Symbolic dynamics was used to analyze some special cases of the three-body problem: Alexeyev [2, 3, 4, 5] has found an intermittence of motions of different types in the one special case of the three-body problem - Sitnikov problem. Symbolic dynamics was also applied in two other special cases of the three-body problem: the rectilinear problem (Tanikawa & Mikkola [10, 11]); and the isosceles problem (Zare & Chesley [14, 6]). Tanikawa & Mikkola [12] considered the case with non-zero angular momentum; they also studied free-fall case and have found sequences of triple collision orbits and periodic orbits for isosceles and collinear cases [13].

It is not easy to visualize initial conditions in the general case because of the high dimension of the problem: 3 masses of the bodies + 9 initial coordinates + 9 initial velocities. Equal-mass free-fall three-body problem is much easier and convenient for study: it drastically reduces the dimension of the problem and allows easy visualization of initial configuration. All the masses are equal, so all permutations of the bodies will give us equivalent systems. Since initial velocities are zero, the problem becomes flat, and at any moment of time we have only two components of coordinates and velocities for each body. If at the initial moment we place two bodies in the points $(-0.5; 0)$ and $(0.5; 0)$, then all possible configurations will be covered if we place the third body inside the region D bounded by two

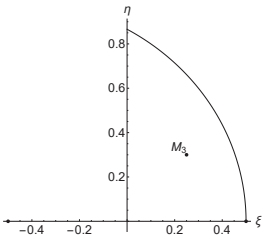


FIGURE 1. Agekian-Anosova region D.

straight line segments and arc of the unit circle centered at $(-0.5, 0)$ (Fig. 1) [1]. All other possible initial configurations (with zero initial velocities) can be received by the projection to this region D and (if needed) transformation of time.

We used code by Seppo Mikkola (Tuorla Observatory, University of Turku) [8] for numerical simulations.

Typical final stage of the evolution of three-body system is close binary moving in one direction, while the third body moves in the opposite direction. So, of interest is finite segment of the symbolic sequences while (infinite) final parts of these sequences are predictable (the only difference is which of the bodies is ejected). If one will calculate entropy of such "infinite" sequence, the result is obvious. So, we study the evolution of the system during the finite period of time (anyway, we can not integrate it infinitely long), considering the stage of active interaction between the bodies. This way, we study complexity of finite sequences and in our "numerical symbolic dynamics" approach we replace original three-body system by a dynamical system that behaves like our original system during this period of time, and have similar behavior all other time (without disruption).

We scan region D with step 0.0005 on each coordinate. For each starting point we numerically integrate equations of motion, construct symbolic sequences and estimate entropy of each sequence. One can use different methods to construct symbolic sequences (see e.g. [9]). In this study, we construct symbolic sequences using binary encounters (we detect minimum distance between two bodies, and corresponding symbol is the number of the distant body, i.e. symbols are from the alphabet {1, 2, 3}), triple encounters (we detect minimum of the sum of all three mutual distances between bodies, corresponding symbol is the number of the distant body, again symbols are from the alphabet {1, 2, 3}), using collinear configuration (similar to [13] we detect the moment when one body crosses the line connecting two distant bodies, there are 6 different configurations possible) and projection to the Agekian-Anosova region D (in [7] authors call it homology mapping – there are 6 possible combinations of projecting our three bodies to the region D, thus the alphabet in this case is {1, 2, 3, 4, 5, 6}).

We also estimate Kolmogorov-Sinai entropy using same approach as in [7] – study spreading of projection of neighboring trajectories on the homology map,

but while in [7] authors used a "drop" consisting of 100 initial points, we use only nine points (point under consideration and 8 neighbours around it in our grid of initial conditions).

References

[1] Agekian, T.A. and Anosova, J.P. 1967, Astron. Zh., 44, 1261

[2] Alexeyev, V. M. 1968a, Math. sbornik, 76, 72

[3] Alexeyev, V. M. 1968, Math. sbornik, 77, 545

[4] Alexeyev, V. M. 1969, Math. sbornik, 78, 3

[5] Alexeyev, V. M. 1981, Uspekhi math. nauk, 36, 161

[6] Chesley, S. 1999, Celest. Mech. Dyn. Astron., 73, 291

[7] Heinämäki, P., Lehto, H., Valtonen. M., and Chernin A., 1999, MNRAS, 310, 811

[8] Mikkola, S. and Tanikawa, K. 1999, Celest. Mech. Dyn. Astron., 74, 287-295.

[9] Mylläri, A., Orlov, V., Chernin, A., Martynova, A. and Mylläri, T. 2016, Baltic Astronomy, vol. 25, 254

[10] Tanikawa, K. and Mikkola, S. 2000a, Cel. Mech. Dyn. Astron., 76, 23

[11] Tanikawa, K. and Mikkola, S. 2000b, Chaos, 10, 649

[12] Tanikawa, K. and Mikkola, S. 2007, in the Proceedings of the Workshop held in St. Petersberg, August 25 - 30, 2007, eprint arXiv:0802.2465, 02/2008

[13] Tanikawa, K. and Mikkola, S. 2015, Publ. Astr. Soc. Japan, vol. 67, No. 6, 115 (1-10)

[14] Zare, K. and Chesley, S. 1998, Chaos, 8, 475

Mylläri Aleksandr
Dept. of Computers & Technology, SAS
St.George's University
St.George's, Grenada, West Indies
e-mail: amyllari@sgu.edu

Mylläri Tatiana
Dept. of Computers & Technology, SAS
St.George's University
St.George's, Grenada, West Indies
e-mail: tmyllari@sgu.edu

Myullyari Anna
Accendo Data LLC
Coral Springs,
Florida, USA
e-mail: anna.myullyari@accendodata.com

Vassiliev Nikolay
V.A. Steklov Institute of Mathematics
of the Russian Academy of Sciences
St. Petersburg, Russia
e-mail: vasiliev@pdmi.ras.ru

Factorization Method for the Second-Order Linear Nonlocal Difference Equations

I.N. Parasidis and E. Providas

Abstract. First, we present solvability criteria and a formula for constructing closed-form solutions to arbitrary second-order linear difference equations with variable coefficients and nonlocal multipoint boundary conditions. Next, we develop an operator factorization method for solving exactly boundary value problems for second-order linear difference equations with polynomial coefficients and containing up to the three boundary points. Of particular relevance here are the references [1, 2, 3].

1. Introduction

Denote by S the linear space of all real-valued functions (sequences) $u_k = u(k)$, $k \in \mathbb{N}$. Let $A : S \to S$ be a second-order linear difference operator defined by

$$Au_k = u_{k+2} + a_k u_{k+1} + b_k u_k, \tag{1.1}$$

where $a_k, b_k, u_k \in S$ and $b_k \neq 0$ for all $k \geq k_1$ or preferably for $k = 1, \ldots$. In addition, let the operator $\widehat{A} : S \to S$ be defined as

$$\widehat{A}u_k = Au_k,$$
$$D(\widehat{A}) = \{u_k \in S : \mu_{i1}u_1 + \mu_{i2}u_2 + \ldots + \mu_{i,l}u_l = \beta_i,\ i = 1, 2,\ l \geq 2\}, \tag{1.2}$$

where μ_{ij}, $\beta_i \in \mathbb{R}$, $i = 1, 2$, $j = 1, \ldots, l$; that is to say $\widehat{A}$ is a restriction of A denoted compactly by $\widehat{A} \subset A$.

Let $u_k^{(1)}, u_k^{(2)}$ be a fundamental solution set of the homogeneous equation $Au_k = 0$ and $u_k^{(f_k)}$ be a particular solution of the non-homogeneous equation

$Au_k = f_k,\ f_k \in S$. Introduce the vector $\mathbf{u}_k^{(H)} = (u_k^{(1)}\ u_k^{(2)})$ and the associated Casorati matrix along with the vectors

$$C_0 = \begin{pmatrix} u_1^{(1)} & u_1^{(2)} \\ u_2^{(1)} & u_2^{(2)} \end{pmatrix}, \quad \mathbf{u}_0 = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}, \quad \mathbf{u}_0^{(f_k)} = \begin{pmatrix} u_1^{(f_k)} \\ u_2^{(f_k)} \end{pmatrix}. \tag{1.3}$$

Furthermore, consider the equation $\widehat{A}u_k = f_k$ for $k = 1, \dots l-3$ together with the two nonlocal boundary conditions and define the $l \times l$ matrix

$$D = \begin{pmatrix} b_1 & a_1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & b_2 & a_2 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \cdots & 0 & \cdots & \cdots & b_{l-2} & a_{l-2} & 1 \\ \mu_{11} & \mu_{12} & \cdots & \cdots & \cdots & \mu_{1,l-2} & \mu_{1,l-1} & \mu_{1,l} \\ \mu_{21} & \mu_{22} & \cdots & \cdots & \cdots & \mu_{2,l-2} & \mu_{2,l-1} & \mu_{2,l} \end{pmatrix}, \tag{1.4}$$

and the vectors

$$\mathbf{u}_l = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_{l-2} \\ u_{l-1} \\ u_l \end{pmatrix} = \begin{pmatrix} \mathbf{u}_0 \\ \mathbf{u}_2 \end{pmatrix}, \quad \mathbf{u}_2 = \begin{pmatrix} u_3 \\ \vdots \\ u_l \end{pmatrix}, \quad \beta_f = \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_{l-2} \\ \beta_1 \\ \beta_2 \end{pmatrix}. \tag{1.5}$$

Then the following theorem holds.

Theorem 1.1. *If* $\det D \neq 0$, *then* $\mathbf{u}_l = D^{-1}\mathbf{b}_f$ *and the nonlocal boundary value problem*

$$\widehat{A}u_k = f_k \tag{1.6}$$

admits a unique solution which can be obtained in closed-form as

$$u_k = u_k^{(f_k)} + \mathbf{u}_k^{(H)} C_0^{-1}(\mathbf{u}_0 - \mathbf{u}_0^{(f_k)}). \tag{1.7}$$

The application of Theorem 1.1 requires the analytic form of two linearly independent solutions and a particular solution of the corresponding homogeneous and non-homogeneous equations, respectively, which may be very difficult to obtain in many cases with variable coefficients. Alternatively, we can use a factorization method.

2. Factorization Method

Definition 2.1. A second-order linear difference operator A defined by (1.1) is said to be factorable when it can be written as a product (composition) of two first-order linear operators A_1, $A_2 : S \to S$, viz.

$$Au_k = A_1 A_2 u_k. \tag{2.1}$$

Lemma 2.2. *An operator A defined by (1.1) is factorable when there exist r_k, $s_k \in S$ such that*

$$Au_k = y_{k+1} + r_k y_k, \tag{2.2}$$

$$A_1 y_k = y_{k+1} + r_k y_k, \quad A_2 u_k = y_k, \tag{2.3}$$

where $y_k = u_{k+1} + s_k u_k$. Moreover, r_k, s_k are a solution of the difference equations

$$\begin{aligned} s_{k+1} + r_k &= a_k, \\ s_k r_k &= b_k. \end{aligned} \tag{2.4}$$

We confine our investigations to the cases where the coefficients a_k, b_k are polynomials and there exist polynomials r_k, s_k which satisfy the system of equations (2.4).

Theorem 2.3. *Let a_k, b_k be polynomials of degree $Deg\, a_k$ and $Deg\, b_k$, respectively. Then the second-order operator A is factorable in the following cases:*

(i) *If $Deg\, a_k < Deg\, b_k$ and there exists a polynomial s_k of degree $Deg\, s_k = 0\, or 1 \ldots or\, Deg\, b_k$ satisfying the equation*

$$s_k s_{k+1} - a_k s_k + b_k = 0, \tag{2.5}$$

or

(ii) *If $Deg\, a_k = Deg\, b_k$ and there exists a polynomial s_k of degree $Deg\, s_k = 0$ or $Deg\, s_k = Deg\, b_k$ satisfying Eq. (2.5),*

Then the polynomial s_k can be constructed by the method of undetermined coefficients and thus $r_k = a_k - s_{k+1}$.

Now we state the main theorem in this paper.

Theorem 2.4. *Let the second-order linear difference operator $\widehat{A}$ defined by (1.2) with $l = 3$, viz.*

$$\begin{aligned} &\widehat{A}u_k = u_{k+2} + a_k u_{k+1} + b_k u_k, \\ &D(\widehat{A}) = \{u_k \in S : \mu_{i1}u_1 + \mu_{i2}u_2 + \mu_{i3}u_3 = \beta_i,\ i = 1, 2\}. \end{aligned} \tag{2.6}$$

Further, let r_k, s_k solve the system of difference equations (2.4). If

$$\det D = \begin{pmatrix} b_1 & a_1 & 1 \\ \mu_{11} & \mu_{12} & \mu_{13} \\ \mu_{21} & \mu_{22} & \mu_{23} \end{pmatrix} \neq 0, \tag{2.7}$$

then,

(i) *The operator $\widehat{A}$ can be factored to $\widehat{A} = \widehat{A}_1\widehat{A}_2$ where the injective first-order operators $\widehat{A}_1$ and $\widehat{A}_2$ are defined by*

$$\widehat{A}_1 y_k = \quad y_{k+1} + r_k y_k = f_k, \quad D(\widehat{A}_1) = \{y_k \in S : y_1 = u_2^* + s_1 u_1^*\}, \tag{2.8}$$

$$\widehat{A}_2 u_k = \quad u_{k+1} + s_k u_k = y_k^*, \quad D(\widehat{A}_2) = \{u_k \in S : u_1 = u_1^*\}, \tag{2.9}$$

where $y_k = u_{k+1} + s_k u_k$, $\widehat{A}u_k = \widehat{A}_1 y_k$, $\mathbf{u}_3^* = col(u_1^*, u_2^*, u_3^*)$, $\mathbf{b}_f = col(f_1, \beta_1, \beta_2)$ and $\mathbf{u}_3^* = D^{-1}\mathbf{b}_f$, and $y_k^* = \widehat{A}_1^{-1} f_k$.

(ii) *The unique solution of the three-point boundary value problem is given in closed-form by*

$$u_k = \widehat{A}^{-1} f_k = \widehat{A}_2^{-1}\widehat{A}_1^{-1} f_k = \widehat{A}_2^{-1} y_k^*. \tag{2.10}$$

Finally, we solve the next example problem.

Example 2.5. The operator $\widehat{A} : S \to S$ defined by

$$\begin{aligned} &\widehat{A}u_k = u_{k+2} - (k+2)u_{k+1} + (k+1)u_k = (k+1)!\,, \\ &D(\widehat{A}) = \{u_k \in S :\ u_1 - u_2 + 2u_3 = 4,\ \ 2u_1 + u_2 + u_3 = 5\}, \end{aligned} \tag{2.11}$$

is injective and the unique solution of (2.11) is given by the formula

$$u_k = \frac{5}{4} + \sum_{j=1}^{k-1} j!\Big(j - \frac{3}{2}\Big) \tag{2.12}$$

3. Conclusion

The technique presented here is simple to use, it can be easily incorporated to any Computer Algebra System (CAS) and more important it can be extended to deal with more complicated problems embracing nonlocal boundary conditions with many points and non-polynomial variable coefficients.

References

[1] A.F. Voevodin, *Factorization method for linear and quasilinear singularly perturbed boundary value problems for ordinary differential equations*, Numer. Analys. Appl. (2009), Vol. 2, No. 1, pp. 1–12.

[2] A.Dobrogowska, G.Jakimowicz, *Factorization method applied to the second order difference equations*, Appl. Math. Lett. (2017), 74, pp. 161–166.

[3] I.N. Parasidis and E. Providas, *Closed-form solutions for some classes of loaded difference equations with initial and nonlocal multipoint conditions*, in *Modern Discrete Mathematics and Analysis*, T. Rassias and N.J. Daras, eds., Springer, 2018.

I.N. Parasidis
Dept. of Electrical Engineering
TEI of Thessaly
41110 Larissa, Greece
e-mail: paras@teilar.gr

E. Providas
Dept. of Mechanical Engineering
TEI of Thessaly
41110 Larissa, Greece
e-mail: providas@teilar.gr

Usage of Automatic Differentiation in Some Practical Problems of Celestial Mechanics

Dmitry Pavlov

Abstract. Building numerically integrated orbits (ephemeris) of celestial bodies has been for a long time an area of celestial mechanics with rich outcome in terms of both science and technology. The model of ephemeris contains a large number of initial parameters and constants that are determined from observations and have an uncertainty. The algorithm requires the first-order derivatives of orbital parameters w.r.t all the determined parameters in the whole timespan of observations. One of the approaches of obtaining those derivatives, examined in this work, is the integration of the derivatives simultaneously with the equations of motion. That requires calculating a function and its partial derivatives w.r.t. a number of parameters at the same time, which is essentially the case for the automatic differentiation technique.

Another usage of the automatic differentiation is the propagation of uncertainty of initial parameters and constants to orbits; the uncertainty, which generally grows with time, can be estimated via the (time-dependent) Jacobian matrix obtained with the numerical integration.

On another note, automatic differentiation allows to build a numerical integrator that is not based on difference schemes like the traditional methods used in celestial mechanics (see papers of Jorba and Zou on Taylor method).

Some preliminary practical results are presented.

Dmitry Pavlov
Laboratory of Ephemeris Astronomy
Institute of Applied Astronomy of the Russian Academy of Sciences
St. Petersburg, Russia
e-mail: dpavlov@iaaras.ru

A sharp version of Shimizu's theorem on entire automorphic functions

Ronen Peretz

Abstract. This paper develops further the theory of the automorphic group of non-constant entire functions. This theory essentially started with two remarkable papers of Tatsujirô Shimizu that were published in 1931. There are three results in this paper. The first result is that the $\mathrm{Aut}(f)$-orbit of any complex number has no finite accumulation point. The second result is an accurate computation of the derivative of an automorphic function of an entire function at any of its fixed points. The third result gives the precise form of an automorphic function that is uniform over an open subset of $\mathbb{C}$. This last result is a follow up of a remarkable theorem of Shimizu. It is a sharp form of his result. It leads to an algorithm of computing the entire automorphic functions of entire functions. The complexity is computed using an height estimate of a rational parameter discovered by Shimizu.

1. Introduction

In 1931 Tatsujirô Shimizu published two remarkable papers having the titles: On the Fundamental Domains and the Groups for Meromorphic Functions. I and II. [2, 3]. There he set up the foundations of the theory of automorphic functions of meromorphic functions. If $f(w)$ is a non-constant meromorphic function then the automorphic functions of f are the solutions $\phi(z)$ of the automorphic equation:

$$f(\phi(z)) = f(z). \tag{1.1}$$

Usually these are many valued functions. They form a group which we denote by $\mathrm{Aut}(f)$. The binary operation being composition of mappings. Most of the results

2010 *Mathematics Subject Classification*: 30B40,30C15,30D05,30D20,30D30,30D99, 30F10,30F35,32D05,32D15
Key Words and Phrases: entire functions, integral functions, meromorphic functions, fundamental domains, automorphic functions of a meromorphic function, the automorphic group of a meromorphic function

of Shimizu in [2, 3], refer to the properties of the individual automorphic functions. In a recent paper, [1], a complementary set of results were obtained. Many of which refer to the global structure of the automorphic group, $\mathrm{Aut}(f)$, rather than to the properties of its individual elements. A very interesting result proved by Shimizu asserts that if the automorphic function $\phi \in \mathrm{Aut}(f)$ is uniform over an open subset of $\mathbb{C}$ (no matter how small), then $\phi(z)$ must be a linear function of the special form $e^{i\theta\pi}z + b$ for some rational $\theta \in \mathbb{Q}$ and some constant $b \in \mathbb{C}$. This result is proven in a sequence of theorems: Theorem 11, Theorem 12, Theorem 13 and Theorem 14. In fact in Theorem 14 Shimizu proves also the converse, i.e. that for any such a function $\phi(z) = e^{i\theta\pi}z + b$, there exists a meromorphic function $f(w)$, such that $\phi \in \mathrm{Aut}(f)$. Shimizu uses in his proofs of these theorems some deep results from the theory of complex dynamics as developed by Fatou and by Julia as well as the Iversen method and well known theorems of Gross and Valiron. There is no indication in Shimizu's theorems as to what are the actual possible values of the arithmetic parameter $\theta \in \mathbb{Q}$. This gap is closed in the current paper where we get an accurate set of possible values of θ in terms of the orders of the zeros of the first derivative of $f(w)$. This enables us to compute an upper bound for the height of Shimizu's parameter θ. An immediate application is an algorithm that computes the entire automorphic functions of $f(w)$. The complexity of this algorithm can easily be estimated using our upper bound for the height of θ. That is the third result of our paper. Its proof relies on our second result, which is the computation of the derivative of an automorphic ϕ at any of its fixed-points. Rather than using the machinery of complex dynamics we invoke an elementary approach that uses calculations with power series. This hard-computational approach has the benefit of being constructive and it gives us effective possible values for $\phi'(z_0)$, for a fixed point $\phi(z_0) = z_0$. That is one of the tools used in our height estimate. Another tool is Theorem 8.4 in [1] which implies that $Z(f') = \mathrm{Fix}(\mathrm{Aut}(f))$. The first result of our paper is really the straight forward observation that the $\mathrm{Aut}(f)$-orbit of any complex number can not have a finite accumulation point. This is immediate by the rigidity property of holomorphic functions. A variant of this was used couple of times by Shimizu. For convenience, we assume in this paper that $f(w)$ is a non-constant entire function. We denote by E the set of all the non-constant entire functions.

2. The main results and their proofs

Proposition 2.1. *Let $f \in E$. Then we have:*
(1) $\forall\, z \in \mathbb{C}$, *the* $\mathrm{Aut}(f)$*-orbit of z, i.e. the set* $\{\phi(z) \,|\, \phi \in \mathrm{Aut}(f)\}$, *(where only those $\phi \in \mathrm{Aut}(f)$ are taken for which $\phi(z)$ is defined) has no finite accumulation point.*
(2) *If $\phi \in \mathrm{Aut}(f)$ has a fixed-point z_0, then either $\phi'(z_0) = 1$ or $f'(z_0) = 0$.*
(3) $\mathrm{Aut}(f) \cap \mathrm{Aut}(f') \subset \{z + b \,|\, b \in \mathbb{C}\}$.

Proof.
(1) If $z \in \mathbb{C}$, $\phi_n \in \mathrm{Aut}(f)$ are such that the elements of the sequence $\{\phi_n(z)\}_n$ are different from one another and $\lim_{n\to\infty} \phi_n(z) = b \in \mathbb{C}$ exists, then: $f(z) = f(\phi_1(z)) = f(\phi_2(z)) = \ldots = f(\phi_n(z)) = \ldots = f(b)$, where the last equality follows by the continuity of f. This implies that $f(w) \equiv f(b)$, a constant. This contradicts the assumption that $f \in E$ and in particular that f is not a constant function.
(2) The automorphic equation $f(\phi(z)) = f(z)$ implies that $\phi(z) \cdot f'(\phi(z)) = f'(z)$. In the last identity we take the limit $z \to z_0$ and recall the assumption $\phi(z_0) = z_0$. The result obtained is $\phi'(z_0) \cdot f'(z_0) = f'(z_0)$. If $f'(z_0) \neq 0$ then $\phi'(z_0) = 1$.
(3) If $\phi \in \mathrm{Aut}(f) \cap \mathrm{Aut}(f')$, then $f(\phi(z)) = f(z)$ and $\phi'(z) \cdot f'(z) = f'(z)$ (by $\phi'(z) \cdot f'(\phi(z)) = \phi'(z) \cdot f'(z)$). Hence $\phi'(z) \equiv 1$. □

Theorem 2.2. *Let $f \in E$, $\phi \in \mathrm{Aut}(f)$ has a fixed-point z_0, and $f'(z_0) = \ldots = f^{(n-1)}(z_0) = 0$, while $f^{(n)}(z_0) \neq 0$. Then:*

$$\phi'(z_0) \in \left\{ e^{2\pi i k/n} \,|\, k = 0, \ldots, n-1 \right\}.$$

Proof.
We use the following expansions about z_0:

$$\phi(z) = z_0 + \phi'(z_0)(z - z_0) + \ldots, \quad \phi'(z) = \phi'(z_0) + \phi''(z_0)(z - z_0) + \ldots,$$

$$f'(z) = \frac{f^{(n)}(z_0)}{(n-1)!}(z - z_0)^{n-1} + \ldots,$$

$$f'(\phi(z)) = f'(z_0 + \phi'(z_0)(z - z_0) + \ldots) = \frac{f^{(n)}(z_0)}{(n-1)!}(\phi'(z_0)(z - z_0) + \ldots)^{n-1} + \ldots.$$

We substitute these into the identity $\phi'(z)f'(\phi(z)) = f'(z)$:

$$(\phi'(z_0) + \phi''(z_0)(z - z_0) + \ldots)\left(\frac{f^{(n)}(z_0)}{(n-1)!}(\phi'(z_0)(z - z_0) + \ldots)^{n-1} + \ldots\right) =$$

$$= \frac{f^{(n)}(z_0)}{(n-1)!}(z - z_0)^{n-1} + \ldots.$$

Equating the coefficients of the lowest non-vanishing power of $(z - z_0)$ which turns up to be $(z - z_0)^{n-1}$ gives:

$$\phi'(z_0)\frac{f^{(n)}(z_0)}{(n-1)!}(\phi'(z_0))^{n-1} = \frac{f^{(n)}(z_0)}{(n-1)!}.$$

Hence $(\phi'(z_0))^n = 1$ which proves the assertion. □

Remark 2.3. Theorem 2.2 is a more accurate version of Proposition 2.1(2).

We can, now, strengthen Theorem 13 on page 247 of [3]. Here is that result:

Theorem 13. [3] *A rational integral function $\Phi(z)$ can not satisfy the equation $f(\Phi(z)) = f(z)$ for a meromorphic (transcendental) function $f(z)$, unless $\Phi(z)$ is*

a linear function of the form $e^{i\theta\pi}z+b$, θ being a rational number.

We also recall that Shimizu demonstrated that if $\Phi \in \mathrm{Aut}(f)$ and if there is an open subset $V \subseteq \mathbb{C}$ over which Φ is uniform, then $\Phi(z) = e^{i\theta\pi}z+b$ for some $\theta \in \mathbb{Q}$ and some $b \in \mathbb{C}$. Thus, the family of these linear functions are the only possible entire functions that qualify as automorphic functions. Here is our sharper version which bounds from above the height of the rational number $\theta \in \mathbb{Q}$ in terms of the orders of the zeros of the derivative $f'(z)$.

Theorem 2.4. *If $f \in E$ and if $\Phi \in \mathrm{Aut}(f)$ and Φ is uniform over some non-empty open subset $\emptyset \neq V \subseteq \mathbb{C}$, then $\Phi(z) = e^{i\theta\pi}z+b$ for some $\theta \in \mathbb{Q}$ and some $b \in \mathbb{C}$ where either $\theta \equiv 0 \mod (2\pi)$ or $\frac{b}{1-e^{i\theta\pi}} \in Z(f')$ in which case if:*

$$f'\left(\frac{b}{1-e^{i\theta\pi}}\right) = \ldots = f^{(n-1)}\left(\frac{b}{1-e^{i\theta\pi}}\right) = 0, \quad f^{(n)}\left(\frac{b}{1-e^{i\theta\pi}}\right) \neq 0,\ n \geq 2,$$

then:

$$\theta \in \left\{ \frac{2k}{n} \,|\, k = 0, 1, \ldots, n-1 \right\}.$$

Proof.
Since $\Phi(z)$ is uniform on some non-empty open subset $\emptyset \neq V \subseteq \mathbb{C}$, it follows by the results of Shimizu mentioned above that $\Phi(z) = e^{i\theta\pi}z+b$ for some $\theta \in \mathbb{Q}$ and some $b \in \mathbb{C}$. If $\theta \not\equiv 0 \mod (2\pi)$ it follows that $e^{i\theta\pi} \neq 1$, and that:

$$\Phi\left(\frac{b}{1-e^{i\theta\pi}}\right) = \frac{b}{1-e^{i\theta\pi}},$$

a fixed-point of the automorphic function $\Phi(z)$. By Theorem 8.4 of [1] we have: $Z(f') = \mathrm{Fix}(\mathrm{Aut}(f))$. Hence:

$$f'\left(\frac{b}{1-e^{i\theta\pi}}\right) = 0.$$

Clearly, there should exist a smallest $n \in \mathbb{Z}^+$, $n \geq 2$ such that:

$$f^{(n)}\left(\frac{b}{1-e^{i\theta\pi}}\right) \neq 0.$$

Otherwise $f(w) \equiv$ Const. which contradicts the assumption $f \in E$. By Theorem 2.2 above we have:

$$\theta \in \left\{ \frac{2k}{n} \,|\, k = 0, 1, \ldots, n-1 \right\}.$$

Theorem 2.4 is now proved. □

Remark 2.5. By Theorem 2.4 it follows that height(θ) is at most equals the order of the zero of the function:

$$f(z) - f\left(\frac{b}{1-e^{i\theta\pi}}\right) \text{ at } z = \left(\frac{b}{1-e^{i\theta\pi}}\right),$$

minus 1.

Thus the following problem is solvable by an algorithm of complexity that could easily be estimated apriori (in the worst case scenario):

Input: An entire function $f \in E$ and a zero z_0 of its derivative, i.e. $f'(z_0) = 0$.

Output: Determine if $f(z)$ has an entire automorphic function $\Phi(z)$ related to z_0. If such an automorphic function exists, then compute it.

The algorithm:
Step 1. Compute the order n of the zero of the function $f(z) - f(z_0)$ at $z = z_0$. It must satisfy $n \geq 2$ by the input.
Step 2. Loop on $k = 1, \ldots, n-1$. For each k compute the complex number $b_k = z_0(1 - e^{2\pi ik/n})$. Check if the following functional equation is satisfied:

$$f(e^{2\pi ik/n}z + b_k) = f(z).$$

If it is satisfied, then output $\Phi(z) = e^{2\pi ik/n}z + b_k$. Stop!
Step 3. Output: "No such an automorphic function exists!".

References

[1] R. Peretz, On the automorphic group of an entire function, submitted for publication, August, 2017.

[2] Tatsujirô Shimizu, On the Fundamental Domains and the Groups for Meromorphic Functions. I, *Japanese journal of mathematics: transactions and abstracts*, Volume **8**, pp 175-236, 1931.

[3] Tatsujirô Shimizu, On the Fundamental Domains and the Groups for Meromorphic Functions. II, *Japanese journal of mathematics: transactions and abstracts*, Volume **8**, pp 237-304, 1931.

Ronen Peretz
Department of Mathematics
Ben Gurion University of the Negev
Beer-Sheva , 84105
Israel
E-mail: ronenp@math.bgu.ac.il

Arithmetic progressions in 2-groups

Fedor Petrov

Let G be a finite group. A subset $A \subset G$ is called progression-free, if $ab = c^2$ for $a, b, c \in A$ implies $a = b = c$. We discuss the maximal possible size $r(G)$ of a progression-free subset of a group G. This subject was initiated by a recent breakthrough paper of E. Croot, V. Lev and P. Pach, where the bound $r(C_4^n) < 3.611^n$ is proved by using the polynomial method. It implies that $r(C_8^n) < 7.222^n$, but using the group rings approach we manage to improve this exponentially. The talk is based on a current work in progress joint with C. Pohoata.

Fedor Petrov
Sankt-Petersburg Department
Steklov Institute of Mathematics
191023, Fontanka 27,
Sankt-Petersburg, Russia
e-mail: fedyapetrov@gmail.com

Notes on character sums and complex functions over finite fields

N. V. Proskurin

Abstract. The intent of this notes is to present briefly the complex functions over finite fields theory. That includes: (a) additive and multiplicative characters; (b) Gauss and Jacobi sums, other trigonometric sums; (c) Fourier expansion, power series expansion, differentiation; (d) special functions like Hermit polynomials, hypergeometric functions and so on. The theory has been developed through parallels with the classical functions theory. The basis for this parallel is the analogy between Gauss sums and the gamma function.

1. Preliminaries

The notation we use is very standard, and we only summarize here the most common. Given prime p, let $\mathbb{F}_q$ be the finite field with $q = p^l$ elements and with prime subfield $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Let trace: $\mathbb{F}_q \to \mathbb{F}_p$ be the trace function. We write $\mathbb{F}_q^\star$ for the multiplicative group of $\mathbb{F}_q$. Fix (once for all) a non-trivial additive character $e_q\colon \mathbb{F}_q \to \mathbb{C}^\star$. With some $h \in \mathbb{F}_q^\star$, one has $e_q(x) = \exp\bigl(2\pi i\,\mathrm{trace}(hx)/p\bigr)$ for all $x \in \mathbb{F}_q$. We write $\widehat{\mathbb{F}}_q^\star$ for the group of multiplicative characters of $\mathbb{F}_q$, i. e. for the group of homomorphisms $\chi\colon \mathbb{F}_q^\star \to \mathbb{C}^\star$. Extend each multiplicative character χ to all of $\mathbb{F}_q$ by setting $\chi(0) = 0$. We write ϵ for the trivial character, $\epsilon(x) = 1$ for all $x \in \mathbb{F}_q^\star$, $\epsilon(0) = 0$. Define $\delta\colon \mathbb{F}_q \to \mathbb{C}$ by setting $\delta(0) = 1$ and $\delta(x) = 0$ for all $x \in \mathbb{F}_q^\star$.

2. Background

The Gauss sum $G(\chi) = \sum\limits_{x\in\mathbb{F}_q^\star} \chi(x)e_q(x)$ with $\chi \in \widehat{\mathbb{F}}_q^\star$, being considered as complex function on $\widehat{\mathbb{F}}_q^\star$, is quite similar to the Euler gamma function

$$\Gamma(s) = \int\limits_0^\infty \exp(-x)\,x^{s-1}dx \quad \text{for} \quad s \in \mathbb{C} \quad \text{with} \quad \mathrm{Re}\,s > 0.$$

For better understanding, note that $x \mapsto \exp(-x)$ is a character of the additive group of real numbers field, that $x \mapsto x^s$ is a character of the multiplicative group of positive real numbers, and that the integration over dx/x is invariant under multiplicative translations. Similarly, we see that the Jacobi sum

$$J(\alpha,\beta) = \sum_{x\in\mathbb{F}_q} \alpha(x)\beta(1-x) \quad \text{with} \quad \alpha,\beta \in \widehat{\mathbb{F}}_q^\star$$

is the analogue of the Euler beta function

$$B(a,b) = \int\limits_0^1 x^{a-1}(1-x)^{b-1}\,dx \quad \text{for} \quad a,b\in\mathbb{C},\ \operatorname{Re} a>0,\ \operatorname{Re} b>0.$$

It occurs that a lot of identities satisfied by the gamma and beta functions have finite field analogues. Say, the formulas

$$G(\chi)\,G(\bar\chi) = \chi(-1)\,q \quad \text{and} \quad J(\alpha,\beta) = \frac{G(\alpha)G(\beta)}{G(\alpha\beta)},$$

where $\chi\neq\epsilon$ and $\alpha\beta\neq\epsilon$, are the finite field analogues of the reflection formula

$$\Gamma(s)\,\Gamma(1-s) = \frac{\pi}{\sin\pi s} \quad \text{for} \quad s\in\mathbb{C}$$

and

$$B(a,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)} \quad \text{with} \quad a,b\in\mathbb{C}.$$

The analogy observed dates back to the nineteenth century. For more advanced analogy we may look on the Gauss multiplication formula for the gamma function,

$$\prod_{n=0}^{m-1} \Gamma\Big(s+\frac{n}{m}\Big) = (2\pi)^{(m-1)/2} m^{1/2-ms}\Gamma(ms)$$

with any $s\in\mathbb{C}$ and integer $m\geq 1$. Given a finite field $\mathbb{F}_q$, a character $\psi\in\widehat{\mathbb{F}}_q^\star$ and an integer $m|(q-1)$, we have a finite field counterpart of the multiplication formula. That is the Davenport–Hasse [1] relation

$$\prod_{\chi} G(\psi\chi) = \Big\{-\bar\psi(m)^m \prod_{\chi} G(\chi)\Big\}\,G(\psi^m),$$

where the products range over $\chi\in\widehat{\mathbb{F}}_q^\star$ under the assumption $\chi^m=\epsilon$.

3. On cubic exponential and Kloosterman sums

A very instructive sample of analogy between classical special functions and character sums is given by Iwaniec and Duke [2]. Consider the integral representation

$$K_{1/3}(u) = u^{1/3}\int\limits_0^\infty \exp\Big(-t-\frac{u^2}{4t}\Big)\frac{dt}{(2t)^{4/3}}$$

for the Bessel–Macdonald function and the Nicholson formula for the Airy integral

$$\int_0^\infty \cos(t^3+tv)\,dt = \frac{v^{1/2}}{3}\,K_{1/3}(2(v/3)^{3/2}),$$

which are valid at least for real positive u, v. From these two formulas, it follows

$$\int_{-\infty}^{\infty} \exp\bigl(i\,(cx^3+x)\,\bigr)\,dx = 3^{-1/2}\int_0^\infty \Bigl(\frac{x}{c}\Bigr)^{1/3} \exp\Bigl(-x-\frac{1}{27cx}\,\Bigr)\frac{dx}{x}$$

with any real $c>0$. Assume $3|(q-1)$. This case there exists cubic character ψ of $\mathbb{F}_q^\star$ and cubic Kloosterman sums, which one can treat as analogue of the integral in the right-hand side. Following the analogue, Iwaniec and Duke deduced very important formula which relates cubic Kloosterman sum to cubic exponential sum. That is

$$\sum_{x\in\mathbb{F}_q} e_q(cx^3+x) = \sum_{x\in\mathbb{F}_q^\star} \psi(xc^{-1})\,e_q(x-(27cx)^{-1}) \quad \text{for} \quad c\in\mathbb{F}_q^\star.$$

The proof in [2] involves Davenport–Hasse relation and Fourier transform. For extended result see [3].

4. Elements of analysis

Consider the complex vector space Ω_q of all functions $\mathbb{F}_q\to\mathbb{C}$ supplied with the inner product

$$\langle f,g\rangle = \sum_{x\in\mathbb{F}_q} f(x)\overline{g(x)} \quad \text{for all} \quad f,g\in\Omega_q.$$

The additive characters form an orthogonal bases for the Ω_q. Given a function $F\colon \mathbb{F}_q\to\mathbb{C}$, its additive Fourier transform is the function $\hat{F}\colon \mathbb{F}_q\to\mathbb{C}$ defined by

$$\hat{F}(x) = \sum_{y\in\mathbb{F}_q} F(y)e_q(yx) \quad \text{for all } x\in\mathbb{F}_q.$$

The Fourier inversion formula

$$F(z) = \frac{1}{q}\sum_{x\in\mathbb{F}_q} \hat{F}(x)e_q(-xz) \quad \text{for all } z\in\mathbb{F}_q$$

allows one to recover F from $\hat{F}$ and can be considered as the expansion of F over basis consisting of additive characters.

Given a function $F\colon \mathbb{F}_q^\star\to\mathbb{C}$, its multiplicative Fourier transform is the function $\widehat{F}\colon \widehat{\mathbb{F}}_q^\star\to\mathbb{C}$ defined by

$$\widehat{F}(\chi) = \sum_{x\in\mathbb{F}_q^\star} F(x)\chi(x) \quad \text{for all } \chi\in\widehat{\mathbb{F}}_q^\star.$$

The Fourier inversion formula

$$F(z) = \frac{1}{q-1} \sum_{\chi \in \widehat{\mathbb{F}}_q^\star} \widehat{F}(\chi)\bar{\chi}(z) \quad \text{for all } z \in \mathbb{F}_q^\star$$

allows one to recover F from $\widehat{F}$. Given a function $F\colon \mathbb{F}_q \to \mathbb{C}$, one has a similar expansion with one additional term

$$F(z) = F(0)\,\delta(z) + \sum_{\chi \in \widehat{\mathbb{F}}_q^\star} C_\chi\,\chi(z) \quad \text{with} \quad C_\chi = \frac{1}{q-1}\,\widehat{F}(\bar{\chi}).$$

One can treat the sum over χ as the sum over $\epsilon, \rho, \rho^2, \dots \rho^{q-1}$, whenever ρ generates the group $\widehat{\mathbb{F}}_q^\star$. So, that is a finite field analogue of power series expansion. The multiplicative characters together with δ form an orthogonal bases for the Ω_q.
For example, given $\rho \in \widehat{\mathbb{F}}_q^\star$ and $x \in \mathbb{F}_q$, one has the expansion

$$\rho(1+x) = \delta(x) + \frac{q}{q-1} \sum_{\chi \in \widehat{\mathbb{F}}_q^\star} \binom{\rho}{\chi} \chi(x) \quad \text{with} \quad \binom{\rho}{\chi} = \frac{\chi(-1)}{q} J(\rho, \bar{\chi}),$$

which is finite field analogue of the classical binomial formula

$$(1+x)^r = \sum_{k=0}^{r} \binom{r}{k} x^k \quad \text{with} \quad \binom{r}{k} = \frac{r!}{(r-k)!\,k!}, \quad x \in \mathbb{C}.$$

For another example, let F be additive character e_q. One has

$$e_q(-z) = 1 + \frac{q}{q-1} \sum_{\chi \in \widehat{\mathbb{F}}_q^\star} \frac{\chi(z)}{G(\chi)} \quad \text{for all} \quad z \in \mathbb{F}_q.$$

That is a finite field analogue for the power series expansion for the exponent. We refer to Greene [4] for both examples and for properties of the binomial coefficients.

5. Differentiation

Given character $\chi \in \widehat{\mathbb{F}}_q^\star$, define the linear operator $D^\chi\colon \Omega_q \to \Omega_q$ by

$$D^\chi F(x) = \frac{1}{G(\bar{\chi})} \sum_{t \in \mathbb{F}_q} F(t)\,\bar{\chi}(x-t)$$

for all $F\colon \mathbb{F}_q \to \mathbb{C}$ and $x \in \mathbb{F}_q$. We find easily

$$D^\epsilon F(x) = F(x) - \sum_{t \in \mathbb{F}_q} F(t),$$

$$\frac{1}{G(\chi)} D^\chi F(x) = \frac{1}{q} \sum_{t \in \mathbb{F}_q} F(t)\,\bar{\chi}(t-x)$$

for all F and x as above and $\chi \neq \epsilon$. According to Evans [5], $D^\chi F$ is the derivative of order χ of F. This definition is motivated by the Cauchy integral formula

$$\frac{1}{n!}\, f^{(n)}(x) = \frac{1}{2\pi i} \int \frac{f(t)\, dt}{(t-x)^{n+1}}$$

for the derivative $f^{(n)}$ of any order n of the function f.
One finds easily some standard properties. Say, D^χ takes constant functions to zero function, whenever $\chi \neq \epsilon$. Then, $D^\alpha D^\beta = D^{\alpha\beta}$ for characters α, β subject to $\alpha\beta \neq \epsilon$. Also, given two functions E and F, $x \in \mathbb{F}_q$, and the character ν we have the formula for integration by parts

$$\sum_{x\in\mathbb{F}_q} E(x)\, D^\nu F(x) = \nu(-1) \sum_{x\in\mathbb{F}_q} F(x)\, D^\nu E(x)$$

and the Leibniz rule for the ν-th derivative of the product

$$D^\nu EF(x) = \frac{1}{q-1} \sum_{\mu\in\widehat{\mathbb{F}}_q^\star} \frac{G(\bar\mu)G(\mu\bar\nu)}{G(\bar\nu)}\, D^\mu E(x)\, D^{\nu\bar\mu} F(x).$$

Given any character ν, let $F(x) = e_q(-x)$ for all $x \in \mathbb{F}_q$. This case we have $D^\nu F = F$. For any function $F\colon \mathbb{F}_q \to \mathbb{C}$ and $a \in \mathbb{F}_q$, we have expansion

$$F(x) = \frac{1}{q-1} \sum_{\nu\in\widehat{\mathbb{F}}_q^\star} G(\bar\nu) D^\nu F(a)\, \nu(a-x)$$

for all $x \in \mathbb{F}_q$, $x \neq a$. That is a finite field analogue of the Taylor expansion.

6. Hermite character sums

Given any character $\nu \in \widehat{\mathbb{F}}_q^\star$, let

$$H_\nu(x) = \frac{1}{G(\bar\nu)} \sum_{u\in\mathbb{F}_q} \bar\nu(u) e_q(u^2 + 2ux) \quad \text{for all} \quad x \in \mathbb{F}_q.$$

The definition is given in [5] as finite field analogue of the classical Hermite polynomials. We find in [5] a lot of formulas involving the character sums H_ν which are quite similar to that for the Hermite polynomials H_n. Say, we have $H_n(-x) = (-1)^n H_n(x)$ for all $x \in \mathbb{R}$ and integer $n \geq 0$, and we have $H_\nu(-x) = \nu(-1)\, H_\nu(x)$ for all $x \in \mathbb{F}_q$, $\nu \in \widehat{\mathbb{F}}_q^\star$. Also, for all $x \in \mathbb{F}_q$, one has

$$H_\nu(x) = \nu(-1) F(x)^{-1} D^\nu F(x), \quad \text{where} \quad F(x) = e_q(x^2).$$

That is a finite field analogue of the Rodriguez formula

$$H_n(x) = (-1)^n \exp(x^2) \frac{d^n}{dx^n} \exp(-x^2), \quad x \in \mathbb{R},$$

for the classical Hermite polynomials H_n.
In a similar manner one can treat the Legendre polynomials, the Bessel functions and other classical polynomials and special functions.

7. Hypergeometric functions

For the hypergeometric function ${}_2F_1$ one has the Euler integral representation

$$ {}_2F_1(a,b;c;x) = \frac{\Gamma(c)}{\Gamma(b)\,\Gamma(c-b)} \int\limits_0^1 t^b (1-t)^{c-b} (1-xt)^{-a} \frac{dt}{t\,(1-t)}. $$

Greene [4] defined the hypergeometric functions on $\mathbb{F}_q$ by

$$ {}_2F_1\Big[\begin{matrix}\alpha,\ \beta\\ \gamma\end{matrix}\Big|\, x\Big] = \epsilon(x)\,\frac{\beta\gamma(-1)}{q} \sum_{t\in\mathbb{F}_q} \beta(t)\,\bar{\beta}\gamma(1-t)\,\bar{\alpha}(1-xt) $$

for any characters $\alpha,\beta,\gamma \in \widehat{\mathbb{F}}_q^\star$ and $x \in \mathbb{F}_q$. With this definition and notation one has power series expansion

$$ {}_2F_1\Big[\begin{matrix}\alpha,\ \beta\\ \gamma\end{matrix}\Big|\, x\Big] = \frac{q}{q-1} \sum_{\chi\in\widehat{\mathbb{F}}_q^\star} \binom{\alpha\chi}{\chi}\binom{\beta\chi}{\gamma\chi}\chi(x), $$

and one has the more general definition

$$ {}_{n+1}F_n\Big[\begin{matrix}\alpha_0,\,\alpha_1,\ldots,\alpha_n\\ \beta_1,\ldots,\beta_n\end{matrix}\Big|\, x\Big] = \frac{q}{q-1} \sum_{\chi\in\widehat{\mathbb{F}}_q^\star} \binom{\alpha_0\chi}{\chi}\binom{\alpha_1\chi}{\beta_1\chi}\cdots\binom{\alpha_n\chi}{\beta_n\chi}\chi(x) $$

for any integer $n \geq 1$ and characters $\alpha_0,\ldots\beta_n \in \widehat{\mathbb{F}}_q^\star$.
Like their classical counterparts, hypergeometric functions over finite fields satisfy many transformation identities. Say, as analogue for Pfaff's transformation [6], [4] we have

$$ {}_2F_1\Big[\begin{matrix}\alpha,\ \beta\\ \gamma\end{matrix}\Big|\, x\Big] = \bar{\beta}(1-x)\,{}_2F_1\Big[\begin{matrix}\bar{\alpha}\gamma,\ \beta\\ \gamma\end{matrix}\Big|\, \frac{x}{x-1}\Big] $$

for any characters $\alpha,\beta,\gamma \in \widehat{\mathbb{F}}_q^\star$ and $x \in \mathbb{F}_q$, $x \neq 1$.
Let us turn to the function ${}_3F_2$. In the classical context, there are some summation formulas. We mean the formulas of Saalschütz, Dixon, Watson, Whipple. Greene [4] gives analogues for each of them. Say, as analogue for Saalschütz's formula [6] we have

$$ {}_3F_2\Big[\begin{matrix}\alpha,\ \ \beta,\ \ \ \gamma\\ \rho,\ \ \alpha\beta\gamma\bar{\rho}\end{matrix}\Big|\, 1\Big] = \beta\gamma(-1)\binom{\gamma}{\bar{\alpha}\rho}\binom{\beta}{\bar{\gamma}\rho} - \frac{1}{q}\beta\rho(-1)\binom{\bar{\beta}\rho}{\alpha}. $$

As one more example, consider Clausen's famous classical identity [7]

$$ {}_3F_2(2c-2s-1,2s,c-1/2;2c-1,c;x) = {}_2F_1(c-s-1/2,s;c;x)^2, $$

which was utilized in de Branges' proof of the Bieberbach conjecture. By Evans and Greene [8], one has a finite field analogue of this formula. That is

$$ {}_3F_2\Big[\begin{matrix}\bar{\alpha}^2\gamma^2,\ \ \alpha^2,\ \ \gamma\phi\\ \gamma^2,\ \ \gamma\end{matrix}\Big|\, x\Big] = -\frac{\bar{\gamma}(x)\,\phi(1-x)}{q} + \frac{\bar{\gamma}(4)\,J(\alpha\bar{\gamma},\alpha\bar{\gamma})}{J(\alpha,\alpha)}\,{}_2F_1\Big[\begin{matrix}\bar{\alpha}\gamma\phi,\ \alpha\\ \gamma\end{matrix}\Big|\, x\Big]^2, $$

where $x \in \mathbb{F}_q$, $x \neq 1$, ϕ is the quadratic character ($\phi \neq \epsilon$, $\phi^2 = \epsilon$), and it is assumed that $\gamma \neq \phi$, $\alpha^2 \neq \epsilon, \gamma, \gamma^2$.

A study of special function analogues over finite fields serve as a useful tool when applied to problems related to character sums. For more transformation formulas, farther developments and applications we refer to [9, 10, 11, 12, 13, 14, 15]. One can find Magma code to compute the hypergeometric functions over finite fields in the dissertation [10].

References

[1] H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. reine angew. Math., **172**, 1934, 151–182.

[2] W. Duke and H. Iwaniec, *A relation between cubic exponential and Kloosterman sums*, Contemporary Mathematics, **143**, 1993, 255–258.

[3] Zhengyu Mao, *Airy sums, Kloosterman sums, and Salié sums*, Journal of Number Theory, **65**, 1997, 316–320.

[4] J. Greene, *Hypergeometric functions over finite fields*, Transactions of the American Math. Soc., **301**, No. 1, 77–101, 1987.

[5] R. J. Evans, *Hermite character sums*, Pacific Journal of Mathematics, **122**, No. 2, 357–390, 1986.

[6] L. Slater, *Generalized hypergeometric functions*, Cambridge Univ. Press, 1966.

[7] W. N. Bailey, *Generalized hypergeometric series*, Strechert–Hafner, New York, 1964.

[8] R. Evans, J. Greene, *Clausen's theorem and hypergeometric functions over finite fields*, Finite Fields and Their Applications **15**, 2009, 97–109.

[9] J. Greene, D. Stanton, *A character sum evaluation and Gaussian hypergeometric series*, Journal of Number Theory, **23**, no. 1, 136–148, 1986.

[10] C. Lennon, *Arithmetic and analytic properties of finite field hypergeometric functions*, Submitted for the degree of PhD at the Massachusetts Inst. of technology, June 2006.

[11] J. Rouse, *Hypergeometric functions and elliptic curves*, Ramanujan Journal, **12**, no. 2, 197–205, 2006.

[12] R. Barman, G. Kalita *Elliptic curves and special values of Gaussian hypergeometric series*, Journal of Number Theory, **133**, issue 9, pages 3099–3111, September 2013.

[13] A. Deines, J. G. Fuselier, L. Long, H. Swisher, Fang-Ting Tu, *Hypergeometric series, truncated hypergeometric series, and Gaussian hypergeometric functions*, Directions in Number Theory, Springer, Cham. Association for women in mathematics series, vol. 3, 2016.

[14] J. Fuselier, L. Long, R. Ramakrishna, H. Swisher, Fang-Ting Tu, *Hypergeometric functions over finite fields*, arXiv:1510.02575v2 [math.NT], 1 April 2016.

[15] R. Evans, J. Greene, *A quadratic hypergeometric ${}_2F_1$ transformation over finite fields*, Proc. Amer. Math. Soc. **145**, 2017, 1071–1076.

N. V. Proskurin
St. Petersburg Department of Steklov Institute of Mathematics RAS
191023, Fontanka 27, St. Petersburg, Russia
e-mail: np@pdmi.ras.ru

Computational Linear and Commutative Algebra

Lorenzo Robbiano

A new book written with Martin Kreuzer will be described in my talk.

• *From the back cover of the book:*

This book combines, in a novel and general way, an extensive development of the theory of families of commuting matrices with applications to zero-dimensional commutative rings, primary decompositions and polynomial system solving. It integrates the *Linear Algebra of the Third Millennium*, developed exclusively here, with classical algorithmic and algebraic techniques. Even the experienced reader will be pleasantly surprised to discover new and unexpected aspects in a variety of subjects including eigenvalues and eigenspaces of linear maps, joint eigenspaces of commuting families of endomorphisms, multiplication maps of zero-dimensional affine algebras, computation of primary decompositions and maximal ideals, and solution of polynomial systems.

This book completes a trilogy initiated by the uncharacteristically witty books Computational Commutative Algebra 1 and 2 by the same authors. The material treated here is not available in book form, and much of it is not available at all. The authors continue to present it in their lively and humorous style, interspersing core content with funny quotations and tongue-in-cheek explanations.

• *From the review of David A. Cox:*

– This book is a lovely blend of commutative and linear algebra.

– The book contains many new results and concepts, along with known ideas drawn from a widely scattered literature.

References

[1] M. Kreuzer and L. Robbiano, *Computational Linear and Commutative Algebra*. Springer, 2016

Lorenzo Robbiano
Dipartimento di Matematica
Università di Genova
Genova, Italy
e-mail: lorobbiano@gmail.com

Confluent Heun equation and equivalent first-order systems

A.A. Salatich and S. Yu. Slavyanov

Introduction

Presented text is an enlargement and elaboration of other publication of the authors [1]. The new vector formulations of confluent Heun equation (further CHE) is proposed. In its turn the text specifies integral symmetries and relation to Painleve equations as obtained in [2].

Consider CHE with two Fuchsian singularities at finite points z_j, $j = 1, 2$ and an irregular singularity at infinity. It reads

$$L^1(D, z)w(z) = (\sigma(z)D^2 + \tau(z)D + (\omega(z) - th))w(z) = 0, \tag{1}$$

Here either

$$\begin{aligned} \sigma(z) &= z(z-1) \\ \tau(z) &= -z(z-1) + c(z-1) + dz \\ \omega(z) &= -az \end{aligned} \tag{2}$$

or

$$\begin{aligned} \sigma(z) &= z(z-t) \\ \tau(z) &= -z(z-t) + c(z-t) + dz \\ \omega(z) &= -az \end{aligned} \tag{3}$$

In both cases (2), (3) polynomials $\sigma(z)$ and $\tau(z)$ are of second degree in z. As the result, differential operator L^1 has dimension 1 according to [3]. Note that the chosen form of CHE (1), (2) corresponds to that in the book [4] however (1), (3) is different from it. The advantage of the latter presentaton is discussed in [1].

Parameter h is called the **accessory parameter**. The chosen factor in front of it, namely t, leads to to the following lemma.

Lemma 1. *Equation (1) with (3) is reduced to confluent hypergeometric equation at $t = 0$.*

Proof. Set $t = 0$ in (1) with (3). We obtain instead of (1) the confluent hypergeometric equation.

At choosing another factor not proportional t, the accessory parameter h is conserved in limiting equation.

The interest to CHE is growing in last decades [4, 5]. Firstly, it is more general comparative to confluent hypergeometric equation. Secondly, more and more physical applications arise.

Linear first order system

The confluent Heun equation can be linked to first-order linear systems. However, these links can be different. One possible way of choosing such a system is determined by the demand that the the residues at Fuchsian points have zero determinant. In the other approach traces of these residues are taken to be zero. We study the first case here. Let the first-order system be

$$Y'\vec{(}z) = A(z)Y\vec{(}z), \quad T(z) = \sigma(z)A(z) \tag{4}$$

where

$$A(z) = \frac{A^{(1)}}{z} + \frac{A^{(2)}}{z-t} + A^{(\infty)} \tag{5}$$

with

$$A^{(1)} = \begin{pmatrix} 0 & 0 \\ h & \theta_1 \end{pmatrix} \quad A^{(2)} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & \theta_2 - a_{11} \end{pmatrix} \quad A^{(\infty)} = \begin{pmatrix} t & 0 \\ 0 & 0 \end{pmatrix}$$

The condition

$$\det A^{(2)} = 0$$

implies

$$a_{11}(\Theta_2 - a_{11}) - a_{21}a_{12} = 0$$

Hence, we arrive to the following result for matrix T

$$T(z) = \begin{pmatrix} a_{11}z + tz(z-t) & a_{12}z \\ h(z-t) + a_{21}z & \theta_1(z-t) + (\theta_2 - a_{11})z \end{pmatrix} \tag{6}$$

Further computations give

$$\operatorname{tr} T = tz(z-t) + \theta_1(z-t) + \theta_2 z$$

$$\det T = \sigma(z)(a_{11}\theta_1 - a_{12}h - t^2\theta_1 + t(\theta_2 + \theta_1 - a_{11})z)$$

$$T_{12}\left(\frac{T_{11}}{T_{12}}\right)' = tz$$

In view of lemma 1 the matrix element a_{12} should be chosen as

$$a_{12} = t \tag{7}$$

The searched equation for the first component of vector $Y\vec{(}z)$ reads

$$\sigma(z)y_1''(z) + P(z)y_1'(z) + Q(z)y_1(z) = 0 \tag{8}$$

where

$$P(z) = -\sigma(z)\left(ln\frac{T_{12}}{\sigma}\right)' - trT = -tz(z-t) + (\theta_1+1)z + \theta_2(z-t)$$

$$Q(z) = T_{12}\left(\frac{T_{11}}{T_{12}}\right)' + \sigma(z)^{-1}detT =$$

$$zt(\theta_1+\theta_2-a_{11}+1) + a_{11}\theta_1 - th$$

The followinng relations between matrix elements and parameters of equation (1) hold

$$a = a_{11} - \theta_1 - \theta_2, \quad c = \theta_2, \quad d = \theta_1 + 1 \tag{9}$$

Shift in accessory parameter is not essential.

Painlevé equation P^V

Painlevé equation is a nonlinear integrable equation, widely studied and applied in last decades. Recent researches in this field one can find, for instance, in collection of papers [8]. Our interests lay in bijection relation between Heun equations and Painlevé equations. [4, 7].

The approach presented in this paper serves as justification of heuristic antiquantization of Heun equation proposed in previous papers starting with publication in J. Phys. A.: Math. Gen. [9].

We shortly repeat derivation of P^V. The transformation of a Hamiltonian to a Lagrangian consist of transfer from variable μ to variable $\dot{q}$ and transfer from Hamiltonian $H(\mu, q)$ to Lagrangian $\mathcal{L}(\dot{q}, q)$ according to

$$\dot{q} = \frac{\partial H}{\partial \mu} = \frac{2\sigma(q)\mu + \tau(q)}{t}$$

$$\mathcal{L}(\dot{q}, q) = \dot{q}\mu - H(\mu, q) =$$
$$\frac{((t)^{1/2}\dot{q} - (t)^{-1/2}\tau(q))^2}{4\sigma(q)} - \frac{\omega(q)}{t} \tag{10}$$

The corresonding Euler equation is actially P^V however it is not completely equal to traditional form of P^V. In order to find and hence resolve the discrepancy we perform the inverse transformation to variable $q \to qt$. That means returning to traditional form of CHE. We obtain

$$\ddot{q} - \frac{1}{2}\left(\frac{1}{q} + \frac{1}{q-1}\right)\dot{q}^2 + \frac{\dot{q}}{t} - \frac{1}{2t^2}\left[(c^2+1)\frac{q}{q-1} - d^2\frac{q-1}{q}\right] -$$
$$\frac{1}{2}q(q-1)(2q-1) + \frac{q(q-1)}{t}((c+d)-2a) = 0 \tag{11}$$

The derived equation is a subset of Painlevé equation P^V. The discussion of its generality can be found in [4].

References

[1] S. Yu. Slavyanov, A. A. Salatich *Confluent Heun equation and confluent hypergeometric equation*, (in Russian) Zap. Nauchn. Sem. PDMI **462** 93-102, (2017).

[2] A.Ya. Kazakov, S. Yu. Slavyanov, TMPh. **179**, 543-549, (2014).

[3] S. Slavyanov, TMPh., **193**, 401-408, (2017).

[4] S. Slavyanov, W. Lay, *Special functions: A unified theory based on singularities*, Oxford University Press, Oxford - New-York, 2000

[5] Ed. A. Ronveau, *Heun's differential equation* (Oxford New York Tokyo, Oxford University Press), 1995.

[6] S. Slavyanov, D. Shatko, A. Ishkhanyan, T. Rotinyan, TMPh., **189**, 1726-1733 (2016).

[7] S. Yu. Slavyanov, O. L. Stesik, TMPh, **186**, 118-125, (2016).

[8] A. D. Bruno, A. B. Batkin (eds.), *Painleve Equations and Related Topics*, De Gruyter, 2012.

[9] S. Yu. Slavyanov, J. Phys. A, **29**, 7329-7335, (1996).

A.A. Salatich and S. Yu. Slavyanov
Saint Petersburg State University,
Saint Petersburg, Russia
e-mail: s.slavyanov@spbu.ru

Real cubic hypersurfaces containing no line of singular points

Alexandr V. Seliverstov

Abstract. We propose a sufficient condition for the absence of a real line consisting of singular points of the given cubic hypersurface over the field of real numbers. There exist examples when this condition is satisfied. There is also an example when this condition is not necessary.

The Bertini theorem provides a simple probabilistic method to check whether the given hypersurface contains a high-dimensional linear subspace of singular points. On the other hand, it is hard to find an isolated singular point of the given cubic hypersurface. Moreover, if the hypersurface as well as all potential singular points are defined over the field of rational numbers, then its singularity recognition is a NP-complete problem.

Let us consider a projective hypersurface $\mathcal{X}$ with a line of singular points. For example, the Whitney umbrella is a ruled surface defined by the form $x_1^2x_3 - x_2^2x_4$; its singular locus contains a line defining by two equations $x_1 = x_2 = 0$.

Let us consider both projective cubic hypersurface $\mathcal{F}$ and hyperplane $\mathcal{H}$ defined by the forms $f(x_0, \dots, x_n)$ and $h(x_0, \dots, x_n)$, respectively. Let a cubic hypersurface $\mathcal{F}_\mathcal{H}$ be defined by the form $h^2x_{n+1} + f$. The hypersurface $\mathcal{F}_\mathcal{H}$ has a singular point with the homogeneous coordinates $(0 : \dots : 0 : 1)$. In the general case, $\mathcal{F}_\mathcal{H}$ is not a cone.

If the hypersurface $\mathcal{F}$ contains a singular point $P \in \mathcal{F} \cap \mathcal{H}$ with the homogeneous coordinates $(p_0 : \dots : p_n)$, then there exists a line of singular points of the hypersurface $\mathcal{F}_\mathcal{H}$; the line contains the point P. Points of this line have coordinates of the type $(p_0 : \dots : p_n : x_{n+1})$, where x_{n+1} is equal to an arbitrary number.

Contrariwise, if a point $\hat{P}$ of the hypersurface $\mathcal{F}_\mathcal{H}$ with the homogeneous coordinates $(p_0, \dots, p_{n+1})$ is singular, and $\hat{P}$ does not coincide with the point $(0 : \dots : 0 : 1)$, then its projection $P \in \mathcal{F}$ with the homogeneous coordinates

$(p_0, \ldots, p_n)$ is singular too. Without loss of generality, one can assume that $h = x_n$.

$$\begin{array}{lrcl} \forall k < n & \frac{\partial}{\partial x_k}\left(x_n^2 x_{n+1} + f(x_0, \ldots, x_n)\right) & = & \frac{\partial f}{\partial x_k} \\ & \frac{\partial}{\partial x_n}\left(x_n^2 x_{n+1} + f(x_0, \ldots, x_n)\right) & = & 2x_n x_{n+1} + \frac{\partial f}{\partial x_n} \\ & \frac{\partial}{\partial x_{n+1}}\left(x_n^2 x_{n+1} + f(x_0, \ldots, x_n)\right) & = & x_n^2 \end{array}$$

The last equation implies that $p_n = 0$. Thus, for all coordinates, the equations

$$\frac{\partial f}{\partial x_k}\Big|_P = \frac{\partial}{\partial x_k}\left(x_n^2 x_{n+1} + f(x_0, \ldots, x_n)\right)\Big|_{\hat{P}} = 0$$

hold. So, the point P is singular.

In particular, if the hyperplane $\mathcal{H}$ contains no singular point of $\mathcal{F}$, then $\mathcal{F}_\mathcal{H}$ has the unique singular point with homogeneous coordinates $(0 : \cdots : 0 : 1)$.

Next, let the cubic hypersurface $\mathcal{F}$ be defined over the field of real numbers. A smooth point $P \in \mathcal{F}$ is said to be elliptic if it is the isolated real point of the intersection of the hypersurface $\mathcal{F}$ and the tangent hyperplane $\mathcal{T}_P$. A sufficient condition for the absence of a real line L consisting of singular points is the existence of an elliptic point $P \in \mathcal{F}$. Let us prove it by contradiction. Assume there exists a real line of singular points. The line intersects all hyperplanes in the projective space. So, the hyperplane section $\mathcal{T}_P \cap \mathcal{F}$ contains both singular points P and $Q \in \mathcal{T}_P \cap L$. Thus, the section contains a real line PQ. But this contradicts the isolation of the real point P.

If a cubic hypersurface contains two real connected components, then the required point exists. The orientable component bounds the convex domain. Therefore, all points of the orientable component are elliptic points. Moreover, if the orientable component of $\mathcal{F}$ does not intersect the hyperplane $\mathcal{H}$, then the hypersurface $\mathcal{F}_\mathcal{H}$ contains an elliptic point.

There exists an affine cubic surface having no elliptic point. For example, it is true for the monkey saddle defined by the equation $x_1(x_1^2 - 3x_2^2) - x_3 = 0$.

Alexandr V. Seliverstov
Institute for Information Transmission Problems of the Russian Academy of Sciences (Kharkevich Institute)
Moscow, Russia
e-mail: slvstv@iitp.ru

On the Pierce–Birkhoff conjecture and related problems.

Mark Spivakovsky

Let R be a real closed field and $B = R[x_1, \ldots, x_n]$ a polynomial ring over R in n variables.

Definition 0.1. *A function $g : R^n \to R$ is said to be* **piecewise polynomial** *if R^n can be covered by a finite collection of closed semi-algebraic sets P_i, $i \in \{1, \ldots, s\}$ such that for each i there exists a polynomial $g_i \in B$ satisfying $g|_{P_i} = g_i|_{P_i}$.*

Piecewise polynomial functions form a ring, containing B, which is denoted by $PW(B)$.

Consider the ring (contained in $PW(B)$) of all the functions obtained from B by iterating the operations of sup and inf. The Pierce–Birkhoff conjecture was stated by M. Henriksen and J. Isbell in the early nineteen sixties ([1] and [3]):

Conjecture 1. (Pierce-Birkhoff) *If $g : R^n \to R$ is in $PW(B)$, then there exists a finite family of polynomials $g_{ij} \in B$ such that $f = \sup_i \inf_j (g_{ij})$ (in other words, for all $x \in R^n$, $f(x) = \sup_i \inf_j (g_{ij}(x))$).*

In this talk, we will recall the definition of the real spectrum of a ring Σ, denoted by Sper Σ. In the nineteen eighties, generalizing the problem from the polynomial ring to an arbitrary ring Σ, J. Madden proved that the Pierce–Birkhoff conjecture for Σ is equivalent to a statement about an arbitrary pair of points $\alpha, \beta \in$ Sper Σ and their separating ideal $< \alpha, \beta >$; we refer to this statement as the **local Pierce-Birkhoff conjecture** at α, β. In [4] we introduced a stronger conjecture, also stated for a pair of points $\alpha, \beta \in$ Sper Σ and the separating ideal $< \alpha, \beta >$, called the **Connectedness conjecture**, about a finite family of elements $f_1, \ldots, f_r \in \Sigma$. In [6] we introduced a new conjecture, called the **Strong Connectedness conjecture**, and proved that the Strong Connectedness conjecture in dimension $n-1$ implies the strong connectedness conjecture in dimension n in the case when $ht(< \alpha, \beta >) \leq n-1$.

The Pierce-Birkhoff Conjecture for $r = 2$ is equivalent to the Connectedness Conjecture for $r = 1$; this conjecture is called the Separation Conjecture. The

Strong Connectedness Conjecture for $r = 1$ is called the Strong Separation Conjecture. In this talk fix a polynomial $f \in R[x, z]$ where $x = (x_1, \ldots, x_n), z$ are $n+1$ independent variables. We will define the notion of two points $\alpha, \beta \in \mathrm{Sper}\ R[x, z]$ being in **good position** with respect to f. Our main result is a proof of the Strong Separation Conjecture in the case when α and β are in good position with respect to f. We also prove that, given a connected semi-algebraic set $D \subset R^n$, if the number of real roots of f, counted with or without multiplicity, is constant for all $x \in D$ then these roots are represented by continuous semi-algebraic functions $\phi_j : D \to R$.

References

[1] G. Birkhoff and R. Pierce, *Lattice-ordered rings.* Annales Acad. Brasil Ciênc. 28, 41–69 (1956).

[2] M. Henriksen and J. Isbell, *On the continuity of the real roots of an algebraic equation*, Proc. AMS Vol. 4, pp. 431-434, 1953.

[3] M. Henriksen and J. Isbell, *Lattice-ordered rings and function rings.* Pacific J. Math. 11, 533–566 (1962).

[4] F. Lucas, J.J. Madden, D. Schaub and M. Spivakovsky, *On connectedness of sets in the real spectra of polynomial rings*, Manuscripta Math. 128, 505-547, 2009.

[5] F. Lucas, D. Schaub and M. Spivakovsky, *Approximate roots of a valuation and the Pierce-Birkhoff Conjecture*, Ann. Fac. Sci. Toulouse, Mathématique, Série 6, Vol. XXI, Fasc. 2, 259-342, 2012.

[6] F. Lucas, D. Schaub and M. Spivakovsky, *On the Pierce-Birkhoff Conjecture*, Journal of Algebra 435, (2015), 124-158.

[7] J. J. Madden, *Pierce–Birkhoff rings.* Arch. Math. 53, 565–570 (1989).

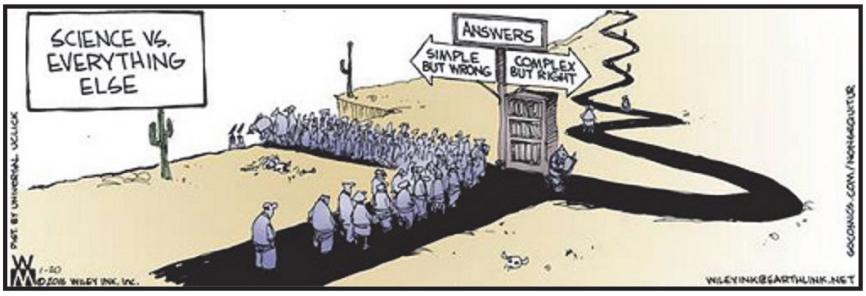
Mark Spivakovsky
CNRS, Institut de Mathématiques de Toulouse 118,
route de Narbonne, F-31062 Toulouse Cedex 9, France
e-mail: mark.spivakovsky@gmail.com

Integration of functions containing parameters and the specialization problem

David R. Stoutemyer, David J. Jeffrey and Robert M. Corless

Abstract. We discuss the calculation and presentation of integrals when parameters are present. We pay special attention to how this is done, or should be done, in tables of integrals and in computer algebra systems. Specifically, we consider two issues: the need for expressions to be *comprehensive* and *continuous*. We present methods for achieving these goals both in manual calculation and in automatic symbolic computation.

Introduction



There are many reference books that publish tables of integrals, for example [1, 3, 6]. An alternative to integral tables is provided by computer algebra systems (CAS), which are already ubiquitous and available on platforms of all sizes. These software systems evaluate integrals using a mixture of integral tables and algebraic algorithms. A feature common to all sources of integrals is the fact that the formulae usually contain parameters. No one wants a table of integrals that contained separate entries for x, x^2 and x^{42}, rather than one entry for x^n, and many tables include additional parameters for user convenience; for example, there will be entries for integrals containing $\sin ax$, rather than the sufficient, but less convenient, $\sin x$.

Although parameters add greatly to the scope and convenience of integral tables, there can be difficulties and drawbacks occasioned by their use. We shall use the word *specialization* to describe the action of substituting specific values (usually numerical, but not necessarily) into a formula. The *specialization problem* is a label for a cluster of problems associated with formulae and their specialization, the problems ranging from inelegant results to invalid ones. For example, in [4] an example is given in which the evaluation of an integral by specializing a general formula misses a particular case for which a more elegant expression is possible. The focus here, however, is on situations in which specialization leads to invalid or incorrect results. To illustrate the problems, consider an example from a fine old Russian textbook [7, ch8, p346, (5)],

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

Expressions equivalent to this are returned by Maple, Mathematica and many other systems, such as the Matlab symbolic toolbox. It is easy to see that the specialization $\sigma = 0$ leaves the integrand in (1) well defined, but the expression for its integral on the right-hand side is no longer defined. If we pursue this further, we see that there are multiple specializations for which (1) fails, *viz.* $\alpha = 0$, $\alpha = 1$, $\lambda = 0$, $\sigma = 0$, $\lambda = -\sigma$, and combinations of these. The question of how or whether to inform computer users of these special cases has been discussed in the CAS literature many times [2]. A list of every special case for (1) is as follows.

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

Conditions are here shown as in printed tables; otherwise they could be presented using the logical $\vee$ and $\wedge$ operators.

To generalize this, we can denote a function depending on parameters by $f(z;\mathbf{p})$, with z being thought of as the main argument, the integration variable, and $\mathbf{p}$ representing the set of parameters. Then (2) is called a comprehensive antiderivative.

Definition 0.1. A *comprehensive antiderivative* of a parametric function $f(z;\mathbf{p})$ is a piecewise function $F(z;\mathbf{p})$ containing explicit consequents[1] for each special case of the parameters.

Computer algebra systems are reluctant to return comprehensive expressions because they can quickly lead to unmanageable computations, and as well many users might regard them as *too much information*. Instead, tables and CAS commonly adopt the approach of identifying a *generic* case, which is then the only expression given; in the case of CAS, the generic case is returned without explicitly showing the conditions on the parameters. In the case of tables, any special case values would be used to simplify the integrand and then the resulting integrand and its antiderivative would be displayed as a separate entry at an appropriate place in the table.

Definition 0.2. A *generic antiderivative* is one expression chosen from a comprehensive antiderivative that is valid for the widest class of constraints.

We have written a Mathematica package that automatically generates comprehensive anti-derivatives for integrands containing parameters.

1. Continuity in parameters

The example (2) dramatically illustrates the potential size of comprehensive antiderivatives, but is too cumbersome for explaining ideas. We turn to simpler examples. We begin with the comprehensive antiderivative known to all students of calculus:

$$\int z^\alpha \,\mathrm{d}z = \begin{cases} \ln z\,, & \text{if } \alpha = -1\,, \\ \dfrac{z^{\alpha+1}}{\alpha+1}\,, & \text{otherwise (generic case)}. \end{cases} \tag{3}$$

Substituting $\alpha = -1$ into the generic case gives $1/0$ and not $\ln z$. Often when a substitution fails, a limit will succeed, so we try the limit as $\alpha \to -1$. This also fails, but we can examine *how* the limit fails by expanding the generic case as a series about $\alpha = -1$, that is treating $\alpha - 1 = \varepsilon$ as a small quantity.

$$\frac{z^{\alpha+1}}{\alpha+1} = \frac{e^{\varepsilon \ln z}}{\varepsilon} = \frac{1 + \varepsilon \ln z + O\left(\varepsilon^2\right)}{\varepsilon}\,. \tag{4}$$

If we can remove the leading term of the series, namely $1/\varepsilon$, then the next term gives us $\ln z$ as desired. But an integral is determined only up to a constant! So,

[1] The expression that is the consequence of specialization.

an equally correct integral is

$$\int z^\alpha \, \mathrm{d}z = \frac{z^{\alpha+1}}{\alpha+1} - \frac{1}{\alpha+1} \ ,$$

and now the limit as $\alpha \to -1$ is exactly $\ln z$. Thus the comprehensive antiderivative [5]

$$\int z^\alpha \, \mathrm{d}z = \begin{cases} \ln z \ , & \text{if } \alpha = -1 \ , \\ \dfrac{z^{\alpha+1}-1}{\alpha+1} \ , & \text{otherwise.} \end{cases} \tag{5}$$

is continuous with respect to α, and the generic antiderivative now contains the exceptional case as a removable discontinuity.

Definition 1.1. Given a function $f(z;\mathbf{p})$ and an expression $F(z;\mathbf{p})$ for the indefinite integral of $f(z;\mathbf{p})$, that is,

$$F(z;\mathbf{p}) = \int f(z;\mathbf{p}) \, \mathrm{d}z \ ,$$

and given a point in parameter space $\mathbf{p}_c$ at which $F(z;\mathbf{p})$ is discontinuous with respect to one or more members of $\mathbf{p}$, a function $C(\mathbf{p})$, which serves as a constant of integration with respect to z, and which has the property that $F(z;\mathbf{p})+C(\mathbf{p})$ is continuous with respect to $\mathbf{p}$ at $\mathbf{p}_c$ is called a Kahanian constant of integration[2].

Definition 1.2. A comprehensive antiderivative in which each consequent contains an appropriate Kahanian constant of integration is a Kahanian antiderivative.

We have written a Mathematica package that computes Kahanian antiderivatives.

References

[1] Milton Abramowitz and Irene A. Stegun. *Handbook of Mathematical Functions: with Formulas, Graphs, and Mathematical Tables*. Dover, 1964.

[2] R. M. Corless and D. J. Jeffrey. Well... it isn't quite that simple. *SIGSAM Bulletin*, 26(3):2–6, 1992.

[3] Izrail Solomonovich Gradshteyn and Iosif Moiseevich Ryzhik. *Table of Integrals, Series, and Products*. Academic Press, 6th edition, 2007.

[4] D. J. Jeffrey and A.D. Rich. Reducing expression size using rule-based integration. In S. Autexier, editor, *Intelligent Computer Mathematics*, volume 6167 of *LNAI*, pages 234–246. Springer, 2010.

[5] W. M. Kahan. Integral of x^n. Personal communication, circa 1959.

[6] Anatolii Platonovich Prudnikov, Yuri A. Brychkov, and Oleg Igorevich Marichev. *Integrals and Series*. CRC Press, 1992.

[2]Since it is a function of $\mathbf{p}$, one can question whether it should be called a constant. It is constant with respect to z, and seems a useful extension of calculus terminology.

[7] Adrian Fedorovich Timofeev. *Integrirovanie funktsii (Integration of Functions).* Publishing House tehniko-teoreticheskoj literature, Leningrad, 1948.

[8] Daniel Zwillinger. *Handbook of Differential Equations.* Academic Press, 3rd edition, 1997.

[9] Daniel Zwillinger. *Standard Mathematical Tables and Formulae.* CRC Press, 32nd edition, 2011.

David R. Stoutemyer
Department Computer Science
University of Hawaii
Honolulu, USA
e-mail: dstout@hawaii.edu

David J. Jeffrey
Dept. Applied Mathematics
University of Western Ontario
London, ON, Canada
e-mail: djeffrey@uwo.ca

Robert M. Corless
Dept. Applied Mathematics
University of Western Ontario
London, ON, Canada
e-mail: rcorless@uwo.ca

Weighted seaweed braids

Alexander Tiskin

Abstract. We continue the algorithmic study of the seaweed monoid (the 0-Hecke monoid of the symmetric group), which has proved to be of fundamental importance for string comparison algorithms. The standard (unweighted) seaweed monoid is parameterised by a natural number n, and consists of $n!$ elements, represented by algebraic objects known as *seaweed braids*. Multiplication of two n-strand seaweed braids results in another n-strand seaweed braid. Such multiplication can be performed in time $O(n \log n)$, and can be used to provide efficient algorithms for various problems on strings and graphs. We consider a generalisation of the seaweed monoid, where each strand of a seaweed braid is assigned a real positive weight. The concept of seaweed braid product can be generalised in a natural way to weighted braids; however, a product of two n-strand weighted seaweed braids may, in general, have more than n weighted strands. We attempt to determine which algebraic and algorithmic properties of unweighted seaweed braids are preserved in the weighted case, and how these properties can be used for problems on weighted strings motivated by biological applications.

References

[1] A. Tiskin. Fast distance multiplication of unit-Monge matrices. *Algorithmica*, 71, 4, pp.859–888, 2015.

[2] A. Tiskin. *Semi-local string comparison: Algorithmic techniques and applications.* `http://arxiv.org/abs/0707.3619`

[3] P. Krusche and A. Tiskin. New algorithms for efficient parallel string comparison. In Proceedings of ACM SPAA, pp. 209—216, 2010.

Alexander Tiskin
Department of Computer Science
University of Warwick
Coventry CV4 7AL, United Kingdom
e-mail: `a.tiskin@warwick.ac.uk`

Reverse Decomposition of Unipotents

Nikolai Vavilov

Abstract. Decomposition of unipotents gives short polynomial expressions of the conjugates of elementary genetators as products of elementaries. It turns out that with some minor twist the decomposition of unipotents can be read backwards, to give very short polynomial expressions of elementary generators in terms of elementary conjugates of an arbitrary matrix and its inverse. For absolute elementary subgroups of classical groups this was recently observed by Raimund Preusser. I discuss various generalisations of these results for exceptional groups, at the relative level, and possible applications.

Decomposition of unipotents [6] was first proposed by Alexei Stepanov for $GL(n, R)$ in 1987, immediately generalised to other split classical groups by the present author, and then further developed in other contexts by a number of authors, see [8, 5, 2] for many further references.

In its simplest form, it can be viewed as a constructive version of the normality of the elementary subgroup. Namely, let Φ be a root system, R be an arbitrary commutative ring with 1, and $G(\Phi, R)$ be the simply connected Chevalley group of type Φ over R. Further, fix a split maximal torus $T(\Phi, R)$ of $G(\Phi, R)$ and the corresponding elementary generators $x_\alpha(\xi)$, where $\alpha \in \Phi$, $\xi \in R$. Let $E(\Phi, R)$ be the elementary subgroup spanned by all these elementary generators.

Then decomposition of unipotents provides explicit polynomial formulae expressing the conjugate $gx_\alpha(\xi)g^{-1}$ of an elementary generator by an arbitrary matrix $g \in G(\Phi, R)$ as a product of elementaries. Thus, for instance, for the groups of types E_6 and E_7 any such conjugate is the product of at most $4 \cdot 27 \cdot 16$ and $4 \cdot 56 \cdot 27$ elementary generators, respectively [7]

Another central classical result in the structure theory of Chevalley groups is description of their normal subgroups, or rather their subgroups normalised by the elementary group $E(\Phi, R)$. What would be an explicit contructive version of that? Until very recently, this was only known in some very special cases. Thus, for $SL(n, \mathbb{Z})$, $n \geq 3$, Joel Brenner [1] established that for an arbitrary matrix $g \in SL(n, \mathbb{Z})$ an elementary transvection $t_{ij}(\xi)$, where ξ belongs to the level of g, is a bounded product of conjugates of g and g^{-1}. Brenner's proof used the theory of elementary divisors, and even generalisations to other groups over PID were

not immediate at all. And of course, there was no hope whatsoever to write such similar formulae for arbitrary commutative rings.

Thus, we were seriously perplexed, when we've first seen the preprints of [3, 4] in Summer 2017. The calculations in [3] start in exactly the same way as in [6], so predictably our assessment of these papers came through the following three stages: 1) There must be nothing new as compared with [6], 2) Gosh, why is it true at all? 3) It is a fantastic breakthrough in the structure theory of algebraic-like groups!

Technically, the twist introduced by Raimund Preusser in the decomposition of unipotents seems to be minor. It consists in expressing a conjugate of an elementary generator not as a product of factors sitting in proper parabolics of certain types, but rather sitting in the products of these parabolics by something small in the unipotent radicals of the opposite parabolics. We were aware of the idea itself [5], but have never appreciated the whole significance of this apparently small variation.

In fact, it allows to reduce degree of the resulting polynomials, and thus both to completely avoid the cumbersome "main lemma", establishing that the coefficients of the occuring polynomials generate the unit ideal, and drastically lower the depth of commutators. In particular, Preusser's idea allows to prove analogues of Brenner's lemma for groups of all types over arbitrary commutative rings, and more.

Immediately after understanding this idea, we were able to generalise it to exceptional groups as well, and to other situations. In particular, it can be derived that for an arbitrary commutative ring R and an arbitrary matrix $g \in G(\Phi, R)$ one can write explicit formulae, expressing an elementary generator $x_\alpha(\xi)$, where ξ belongs to the level of g, as products of at most $8 \cdot dim(G)$ elementary conjugates of g and g^{-1}.

I discuss further development of this idea, such as our joint paper with Zhang Zuhong, where we write similar formulae at the relative level, expressing elementary generators as products of conjugates of g and g^{-1} by elements of the relative elementary subgroups $E(\Phi, R, I)$, corresponding to an ideal $I \trianglelefteq R$. This result has significant applications to the description of subnormal subgroups of $G(\Phi, R)$, etc.

I sketch further imminent applications of these ideas, to description of various classes of intermediate subgroups, the values of word maps, etc.

References

[1] J. L. Brenner, *The linear homogeneous group. III*, Ann. of Math. (2) 71 (1960), 210—223.

[2] V.A. Petrov, *Decomposition of transvections: An algebro-geometric approach,*, Algebra i Analiz 28 (2016), no. 1, 150–157.

[3] R. Preusser, *Sandwich classification for $GL_n(R)$, $O_{2n}(R)$ and $U_{2n}(R, \Lambda)$ revisited*, J. Group Theory 21 (2018), 21–44

[4] R. Preusser, *Sandwich classification for $O_{2n+1}(R)$ and $U_{2n+1}(R,\Delta)$ revisited*, arXiv:1801.00699v1 [math.KT] 2 Jan 2018, 1–20, accepted to J. Group Theory (2018)

[5] A.V.Stepanov, *A new look at the decomposition of unipotents and the normal structure of Chevalley groups*, Algebra i Analiz 28 (2016), no. 3, 161–173.

[6] A. Stepanov and N. Vavilov, *Decomposition of transvections: A theme with variations*, K-Theory 19 (2000), no. 2, 109–153.

[7] N. Vavilov, *A third look at weight diagrams*, Rend. Sem. Mat. Univ. Padova, 104 (2000), 201–250.

[8] N.A. Vavilov, *Decomposition of unipotents for E_6 and E_7: 25 years after*, Zap. Nauchn. Sem. POMI 430 (2014), 32–52.

Nikolai Vavilov
Department of mathematics and Mechanics
St. Petersburg State University
St. Petersburg, Russia
e-mail: nikolai-vavilov@yandex.ru