Table of content

Semjon Adlaj
The generalized arithmetic-geometric mean 7

Alexander Batkhin
Computation of Hamiltonian high order normal form 9

Yuri Blinkov, Rustam Bayramov, Mikhail Malykh
GInv: software for calculation of Gröbner involutive basis 13

Alexander Bruno, Alexander Batkhin, Zafar Khaydarov
Multifrequency resonant conditions in Hamiltonian systems 16

Martin Bures, Arsen Khvedelidze, Dimitar Mladenov, Stanislav Velkov
On basic stratified structures in quantum information geometry 21

Victor Edneral
On the Integrability of the Polynomial Case of the Liénard-type Equation .. 23

Alexandr Grebennikov, Gayane Panina
Around concurrent normal conjecture 27

Sergei Gubanov
Algebraic solution of a scheduling problem in project management 28

Mika Hirvensalo, Nikita Gogin
Riemann Hypothesis Property for The Convergents of a Continued Fraction Expansion 33

Stefan Hypolite James, Tatiana Myllari
Teaching Math in SGU with Computer Algebra Systems 37

Boris Kazarnovskii
Is there an algebraic geometry for exponential sums? 42

Vladimir Kornyak
Symplectic Structures in Finite Quantum Mechanics and Generalized Clifford Algebras 44

Nikolai Krivulin
Tropical optimization techniques for solving multicriteria problems in decision making 46

Nikolai Krivulin, Alexey Prinkov
Solving the problem of choosing an information system project by methods of tropical mathematics 53

Mikhail Malykh
On the computation of Abelian differential of the third kind 59

Ksaverii Malyshev
Fourier series summation and A.N. Krylov convergence acceleration in CAS 63

Andrei Malyutin
Fair division algorithms with a small number of queries 64

Farid Mikhailov
Computing the dimensions of the components of tropical prevarieties 71

Aleksandr Myllari, Tatiana Myllari
Three-body dynamics: Agekian-Anosova region D 77

Gaiane Panina
Around concurrent normals conjecture 81

Fedor Petrov
Hidden symmetry of certain rational functions 82

Nikolai Proskurin
On some numerical experiments with character sums over finite fields 83

Alexander Sakharov
Symbolic Inference for Non-Horn Knowledge Bases With Fuzzy Predicates 86

Alexandr Seliverstov
Generic-Case Complexity of the Multiple Subset Sum Problem 96

Soloviev Sergei
Automorphisms of Types and Cryptography 100

Alexander Tiskin
The Chvatal-Sankoff problem: Understanding random string comparison through stochastic processes 103

Alexander Tiskin
Fast RSK correspondence by doubling search 104

Vladimir Titov
Zero-velocity surfaces in the general three-body problem 105

Astghik Torosyan, Arsen Khvedelidze
Hierarchy of classicality indicators for N-level systems 106

Nikolay Vasilyev
On Groebner bases in semigroup rings of partially ordered semigroups. 108

Nikolai Vavilov, Boris Kunyavskii, Eugene Plotkin
Bounded elementary generation of Chevalley groups 109

Nikolai Vavilov, Vladimir Khalin, Alexander Yurkov
Mathematics for Non-Mathematicians: an Idea and the Project 121

Anatoly Vershik
0-1 laws in asymptotic combinatorics and central markov measures for continuous graphs 150

Dmitry Zaykov, Sergei Pozdniakov
Wise Tasks Graphs System 151

Eugene Zima
Change and Solve 157

The generalized arithmetic-geometric mean

Semjon Adlaj

Abstract. The generalized arithmetic-geometric mean (GAGM) is the "canonical" generalization of the arithmetic-geometric mean (AGM) which was discovered by Gauss to enable most efficient calculation of complete elliptic integrals. It thereby provides the framework necessary for a contemporary Computer Algebra System (CAS), where complete elliptic integrals of all kinds are to be exactly evaluated and robustly, swiftly calculated.

The introduction of the arithmetic-geometric mean (AGM) signified (as Gauss recorded in his diary on May 30, 1799) the emergence of a "new era of analysis" [1]. Yet, over two more centuries were required before the great significance of Gauss' discovery was understood. The concept of the modified arithmetic-geometric mean (MAGM), discussed in [2], clarified the link between the complete elliptic integral of two kinds (the second with the first). The Computer Algebra System (CAS) "MathPartner", which implementation was discussed in [3], incorporates both the AGM and the MAGM, as told in [4, 5].

The GAGM might be regarded as the concept linking to each other complete elliptic integral of all (three) kinds. The procedure for calculating the perimeter of an ellipse via the GAGM, presented in [6], emphasized that the calculation of the complete elliptic integral of the second kind did not necessarily require separate calculations of the AGM and the MAGM. We also emphasized the Gauss-Euler algorithm as the algorithm (with no other namings for this algorithm to be ever justified, contrary to claims made in [7]) underlying fast algorithms for calculating the constant π. Thus, further incorporating the GAGM in CAS "MathPartner" provides the framework necessary for exact and robust calculations of complete elliptic integrals of all kinds, including the third kind, which is notorious to many contemporary CAS for being too prone to erroneous calculations. The errors being unavoidable whenever the multivaludness of (path-dependent) elliptic integrals is not properly addressed. The exploration of the algebraic properties of the GAGM provides the necessary tools for matching its multivaludness with corresponding multivaludness of complete elliptic integrals, with the Galois elliptic function, as defined in [8], providing the basis for such exploration.

This work was supported by the Russian Foundation for Basic Research (Project № 19-29-14141).

References

[1] *Gauß' wissenschaftliches Tagebuch 1796-1814*. Mathematische Annalen 57 (1903): 1-34.

[2] Mathematics Stack Exchange. *Modified Arithmetic-Geometric Mean*. Answered by Francois Lamarche on Oct 5, 2016 and edited on Dec 9, 2019. Available at https://math.stackexchange.com/questions/391382/modified-arithmetic-geometric-mean

[3] Pozdniakov S. *Using Math Partner Environment in Algorithmic Mathematics Course*. 14th International Conference on Polynomial Computer Algebra. Euler International Mathematical Institute, St. Petersburg, April 19–24, 2021. Available at https://pca-pdmi.ru/2021/files/41/pca_example_Pozdniakov.pdf

[4] Malaschonok G. & Seliverstov A. *New Features in MathPartner 2021*. Computer tools in education, 2021, № 3: 29–40. Available at http://www.ipo.spb.ru/journal/content/2286/Новые%20функции%20в%20MathPartner%202021.pdf

[5] Malaschonok G. & Seliverstov A. *Calculation of integrals in MathPartner*. Discrete and Continuous Models and Applied Computational Science, 2021, Vol. 29, № 4: 337-346. Available at https://doi.org/10.22363/2658-4670-2021-29-4-337-346

[6] Adlaj S. *An explicit procedure for calculating the perimeter of an ellipse*. 22nd Workshop on Computer Algebra in memory of Professor Vladimir Gerdt, Dubna, Russia, May 24–25, 2021. Available at https://indico-hlit.jinr.ru/event/187/contributions/1769/attachments/543/931/SAdlaj.pdf

[7] Brent R. *Old and new algorithms for pi*. Letters to the Editor. Notices of the AMS 60(1) (2013): 7. Available at https://www.ams.org/notices/201301/rnoti-p7.pdf

[8] Adlaj S. *Galois elliptic function and its symmetries*. 12th International Conference on Polynomial Computer Algebra. Euler International Mathematical Institute, St. Petersburg, April 15–20, 2019. Available at https://pca-pdmi.ru/2019/files/37/PCA2019SA_slides.pdf

Semjon Adlaj
Department of Mathematics
Division of Complex Physical and Technical Systems Modeling
A.A. Dorodnicyn Computing Center of the Russian Academy of Sciences
Moscow, Russia
e-mail: SemjonAdlaj@gmail.com

Computation of Hamiltonian high order normal form

Alexander Batkhin

Abstract. The procedure of deriving homological equations of arbitrary order, which solutions are used in iterative procedure of normalization of a Hamiltonian in a neighborhood of an equilibrium position, is considered. A formula for a homological equation of arbitrary order used in the method of normalization by means of the Lie series is proposed. The normalization procedure is applied to Hamiltonian of the Hill problem written in scaled regular variables. The resulting normal form of the Hill problem can be used to find domains of analyticity of the normalizing transformation.

Introduction

Normal form (NF) of a system of ordinary differential equations (ODE) computed near an invariant manifold (stationary point, periodic solution or invariant torus) is rather powerful technique for investigation of local dynamics of the phase flow in the vicinity of this invariant structure. Even though the NF is a formal object it can be used for searching first integrals of the system, families of periodic solutions, for studying integrability, stability and bifurcations. The special properties of Hamilton systems require specific algorithms for computation their NF. The goal of the presented work is to provide a procedure for constructing so called homological equation of any order, which is used in the procedure of so called invariant Hamiltonian normalization .

1. Hamiltonian normal form

We consider an analytic Hamiltonian system

$$\dot{\mathbf{x}} = \frac{\partial H}{\partial \mathbf{y}}, \quad \dot{\mathbf{y}} = -\frac{\partial H}{\partial \mathbf{x}} \tag{1}$$

with n degrees of freedom near its stationary point $\mathbf{x} = \mathbf{y} = 0$.

The Hamiltonian function $H(\mathbf{x},\mathbf{y})$ is expanded into convergent power series $H(\mathbf{x},\mathbf{y}) = \sum H_{\mathbf{pq}}\mathbf{x}^{\mathbf{p}}\mathbf{y}^{\mathbf{q}}$ with constant coefficients $H_{\mathbf{pq}}$, $\mathbf{p},\mathbf{q} \geq 0$, $|\mathbf{p}|+|\mathbf{q}| \geq 2$.

Canonical transformations of coordinates $\mathbf{x},\mathbf{y}$

$$\mathbf{x} = \mathbf{f}(\mathbf{u},\mathbf{v}), \quad \mathbf{y} = \mathbf{g}(\mathbf{u},\mathbf{v}), \tag{2}$$

preserve the Hamiltonian character of the initial system (1).

Denoting by $\mathbf{z} = (\mathbf{x},\mathbf{y}) \in \mathbb{R}^{2n}$ the phase vector one can write the linear part of the system (1) in the form

$$\dot{\mathbf{z}} = B\mathbf{z}, \quad B = \frac{1}{2}\, J \operatorname{Hess} H|_{\mathbf{z}=0}\,, \quad J = \begin{pmatrix} 0^n & E^n \\ -E^n & 0^n \end{pmatrix},$$

where J is symplectic unit matrix, E^n is identity matrix and $\operatorname{Hess} H$ is Hessian of function H. Let $\lambda_1,\dots,\lambda_{2n}$ be eigenvalues of the matrix B, which can be reordered in such a way that $\lambda_{j+n} = -\lambda_j$, $j = 1,\dots,n$. Denote by $\boldsymbol{\lambda} = (\lambda_1,\dots,\lambda_n)^{\mathrm{T}}$.

There exists [1, § 12, Theorem 12] a canonical formal transformation (2) in the form of power series, which reduces the initial system (1) into its *normal form* for the case of semi-simple eigenvalues

$$\dot{\mathbf{u}} = \frac{\partial h}{\partial \mathbf{v}}, \dot{\mathbf{v}} = -\frac{\partial h}{\partial \mathbf{u}},$$

defined by the normalized Hamiltonian

$$h(\mathbf{u},\mathbf{v}) = \sum_{j=1}^{n} \lambda_j u_j v_j + \sum h_{\mathbf{pq}}\mathbf{u}^{\mathbf{p}}\mathbf{v}^{\mathbf{q}},$$

containing only resonant terms $h_{\mathbf{pq}}\mathbf{u}^{\mathbf{p}}\mathbf{v}^{\mathbf{q}}$ with

$$\langle \mathbf{p}-\mathbf{q}, \boldsymbol{\lambda}\rangle = 0.$$

Here $0 \leq \mathbf{p},\mathbf{q} \in \mathbb{Z}^n$, $|\mathbf{p}|+|\mathbf{q}| \geq 2$ and $h_{\mathbf{pq}}$ are constant coefficients.

2. Invariant normalization method and its application

Here we describe normalization procedure.

- The real Hamiltonian $H(\mathbf{x},\mathbf{y})$ is written in the complex form $H(\mathbf{z},\bar{\mathbf{z}})$.
- The method of invariant normalization is applied to $H(\mathbf{z},\bar{\mathbf{z}})$ up to the definite order and we get it NF $h(\mathbf{Z},\bar{\mathbf{Z}})$, which contains only resonant terms.
- The obtained complex NF $h(\mathbf{Z},\bar{\mathbf{Z}})$ can be transformed into the real NF $h(\mathbf{X},\mathbf{Y})$.

Here we consider a Hamiltonian system, which stationary point (SP) coincides with the origin. Applying scaling $\mathbf{x} \to \varepsilon\mathbf{x}$, $\mathbf{y} \to \varepsilon\mathbf{y}$ and $t \to \varepsilon^2 t$ one can write it in the form of power series in ε: $H(\mathbf{x},\mathbf{y}) = H^0 + F = H^0 + \sum_{j=1}^{\infty} \varepsilon^j H_j(\mathbf{x},\mathbf{y})$, where H^0 is quadratic (unperturbed) form and H_j is a homogeneous form of order $j+2$. We are looking for the NF of the original Hamiltonian H as a power series $h(\mathbf{z},\bar{\mathbf{z}}) = h^0 + f = h^0 + \sum_{j=1}^{\infty} \varepsilon^j h_j(\mathbf{z},\bar{\mathbf{z}})$, where $h^0 = \sum_{j=1} \lambda_j z_j \bar{z}_j$ and homogeneous forms h_j, $j > 0$, contain only resonant terms $h_{\mathbf{pq}}\mathbf{z}^{\mathbf{p}}\bar{\mathbf{z}}^{\mathbf{q}}$, $|\mathbf{p}|+|\mathbf{q}| = j+2$, such that $\langle \boldsymbol{\lambda}, \mathbf{p}-\mathbf{q}\rangle$. Transformation from the initial Hamiltonian H to its NF h is provided by Lie generator G having form of a power series of ε: $G=\sum_{j=1}\varepsilon^j G_j$: $h = H+\sum_{j=1}^{\infty}\frac{1}{j!}H*G^j$. Lie generator G produces a near identical transformation, so we have $h^0=H^0$ and then

$$f = h^0 * G + M, \quad M = F + \sum_{j=1}\frac{1}{j!}H*G^j. \tag{3}$$

Solution of (3) can be obtained be the *method of invariant normalization*, proposed by V.F. Zhuravlev [2, 3]. This method can be considered as subsequent averaging of functions M_j along the unperturbed solutions $\mathbf{z}(t,\mathbf{Z},\bar{\mathbf{Z}})$ obtained from the unperturbed system with Hamiltonian H^0. It can be applied for the case of nonzero eigenvalues.

According to it the homological equations can be rewritten in the form

$$\frac{df_j}{dt}=0, \quad M_j = f_j - \frac{dG_j}{dt}, \quad j=1,2,\dots \tag{4}$$

Substituting the solutions $\mathbf{z}(t,\mathbf{Z},\bar{\mathbf{Z}})$, $\bar{\mathbf{z}}(t,\mathbf{Z},\bar{\mathbf{Z}})$ to the unperturbed system into the function M_j one gets function $m_j(t,\mathbf{Z},\bar{\mathbf{Z}}) = M_j(t,\mathbf{Z},\bar{\mathbf{Z}})$ and getting the following quadrature

$$\int_0^t m_j(t,\mathbf{Z},\bar{\mathbf{Z}})dt = tf_j(\mathbf{Z},\bar{\mathbf{Z}}) + G_j(\mathbf{Z},\bar{\mathbf{Z}}) + g(t). \tag{5}$$

Hence, on each step of the normalization procedure the next term of the NF f_j equals the coefficient at t, and the Lie generator term G_j equals the time-independent term in (5).

It is possible to reduce approximately in 4 times the number of terms in functions M_j, $j=2,3,\cdots$. From the first equation of (3) for each $j=2,3,\dots$ one can get that $h^0 * G_j = f_j - M_j$. Let us introduce the following notations:

$$f_j^+ \equiv F_j + f_j, f_j^- \equiv F_j - f_j, H*G^k_{j_1\cdots j_k} = H*G^{k-1}_{j_1\cdots j_{k-1}} * G_{j_k}.$$

Statement 1. *For $j>2$ function M_j is constructed in a such way:*

- *Term F_j is taking and sum $\frac{1}{2}\sum\limits_{k=1}^{j-1} f_k^+ * G_{j-k}$ is adding to it.*
- *For each k not greater than $[j/2]$ we compute the set $\mu_{2k+1}(j)$ of all permutations of any partition $\nu_{2k+1}(j)$, i.e. the set $\mu_{2k+1}(j)$ contains the tuple of $2k+1$ indices which sum is equal to j. For each such tuple $(i_1,\dots,i_{2k+1})$ of indices one has to compute all the Poisson brackets of form $f_{i_1}^- * G^{2k}_{i_2\cdots i_{2k+1}}$.*
- *The sum all the computed above Poisson brackets is multiplied by the coefficient α_{2k}. These coefficients are well known Bernoulli numbers B_{2k} divided by factorial $(2k)!$: $\alpha_{2k}=\frac{B_{2k}}{(2k)!}$. They can be computed with the help of generating function $\mathfrak{g}(\varepsilon)=\frac{\varepsilon}{2}+\frac{\varepsilon}{e^{\varepsilon}-1}-1$.*

- *The final formula for M_j can be written as follows*

$$M_j = F_j + \frac{1}{2}\sum_{k=1}^{j-1} f_k^+ * G_{j-k} + \sum_{k=1}^{[j/2]} \alpha_{2k} \sum_{(i_1,\dots,i_{2k+1})\in\mu_{2k+1}^j} f_{i_1}^- * G_{i_2\cdots i_{2k+1}}^{2k}.$$

It is evident that high order normalization of the Hamiltonian H is only possible with computer algebra systems. For example, such software [3, Ch. 7] was developed in CAS `Wolfram Mathematica`. The author implemented the described above algorithm in CAS `Maplesoft Maple`. Nevertheless, this invariant normalization method can be implemented in other open source CAS. For example, in `SageMath`, which essentially uses the `SymPy` symbolic computation package, or `Maxima`.

The method of invariant normalization was applied to the well know planar circular Hill problem, which Hamiltonian written in scaled regularized variables has polynomial form. The NF h in the vicinity of the origin was computed up to the 20-th order. This NF can be used for asymptotic integration of the Hill's problem equations of motion and for studying so called domains of analyticity [4].

References

[1] A.D. Bruno, *Analytical form of differential equations (II)*, Trans. Moscow Math. Soc. 26(1972), 199–239.

[2] V.F. Zhuravlev, *Invariant normalization of non-autonomous Hamiltonian systems*, J. Appl.Math. Mech. 66 (2002), no. 3, 347–355.

[3] V.F. Zhuravlev, A.G. Petrov, M.M. Shunderyuk, *Selected Problems of Hamiltonian Mechanics*, Moscow: LENAND, 2015 [in Russian].

[4] A.D. Bruno, *The Restricted 3-Body Problem: Plane PeriodicOrbits*, Moscow: Nauka, 1990; New York: De Grüyter, 1994.

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`

GInv: software for calculation of Gröbner involutive basis

Yuri A. Blinkov, Rustam E. Bayramov and Mikhail D. Malykh

Abstract. The open source software GINV implements the Gröbner bases method for systems of equations. In the report, a new revised version of GInv will be presented. We use this system for analytical study of cubature formulas on a sphere known as Popov's problem.

The study of systems of nonlinear equations in modern computer algebra systems is based on the calculation of Gröbner bases of ideals generated by the left-hand sides of the equations of these systems. The implementation of the Buchberger algorithm, which came to this system from the Singular system, is used. Buchberger's algorithm is the oldest, the basic version of Buchberger's algorithm leaves a lot of freedom in carrying out the computational process, thus considerable improvements are obtained by implementing criteria for reducing the number of S-polynomials to be actually considered (e.g., by applying the product criterion or the chain criterion).

In the late 1990s, involutive algorithms [1, 2] were proposed as an alternative to the Buchberger algorithm and implemented in the GInv system. On the initiative of V.P. Gerdt and Yu.A. Blinkov in 2005, the GInv project (`http://invo.jinr.ru`) was founded, within which software was developed for calculating involutive bases, written as a C++ module for the Python language. Recently, this system has been significantly revised by one of the authors of this paper, the new version is in the public access and is available at `https://github.com/blinkovua/GInv`. In the new version of the GInv system, dynamic memory reallocation mechanisms have been added, which allow speeding up calculations significantly, up to several times. The proposed approach is fundamentally different from other algorithms known under the general name 'garbage collection' [3] and is based on the implementation of object-oriented programming in C++.

A good demonstration of the achievements of the GInv system was an analytical study of cubature formulas on a sphere known as Popov's problem. The development of the theory of cubature formulas on the sphere that are invariant under transformations of finite symmetry groups of regular polyhedra was the subject of recent studies by A.S. Popov [4]. In Popov's works the solution of the problem is reduced to the study of a system of nonlinear algebraic equations, which was then solved numerically using the computer facilities of the Siberian Supercomputer Center. We investigate the problem of finding the weights and nodes of cubature formulas of a given order on a unit sphere that are invariant under the rotation groups of the icosahedron (described by A.S. Popov's in [5]) using free-access computer algebra systems, namely, the popular general-purpose system Sage (`https://www.sagemath.org`) and the GInv system.

Popov's algorithm for reducing the problem to a system of nonlinear equations is implemented in Sage. For approximation orders 19 and 20, the set of solutions is described using standard tools of the Sage system. For order 23, Popov's problem could not be solved in Sage, since the system could not calculate the Gröbner basis of the ideal for the system of equations describing Popov's problem in this case in a few days. However, the GInv system successfully coped with this task; it turned out that the basis polynomials have extremely large integer coefficients. Further, using the well-known Gröbner basis, it was possible to completely describe the set of solutions to the Popov problem in Sage. The exact solutions found using computer algebra systems are compared with the solutions found numerically by Popov. In particular, a new solution of the Popov problem is found for the order of approximation equal to 23.

It should be emphasized that this test is not artificial, specially invented for testing computer algebra systems, and the results themselves are of general scientific interest. It is impossible not to note the significant difference between the parameters characterizing the calculation of the Gröbner basis when studying the Popov problem and standard tests (`http://invo.jinr.ru/ginv/benchmark.html`): the coefficients of the basis polynomials turn out to be huge, and the degrees on the contrary, remain small.

Acknowledgments. This work is supported by the Russian Science Foundation (grant no. 20-11-20257).

References

[1] Zharkov, A.Y.; Blinkov, Y.A. Solving zero-dimensional involutive systems. In Progress in Mathematics; Birkhauser: Basel, 1996; Vol. 143, pp. 389–399. doi:10.1007/978-3-0348-9104-2_20.

[2] Gerdt, V.P.; Hashemi, A.; M.-Alizadeh, B. Involutive Bases Algorithm Incorporating F5 Criterion. J. Symb. Comput. 2013, 59, 1–20. doi:10.1016/j.jsc.2013.08.002.

[3] Jones, R.; Hosking, A.; Moss, J.E.B. The Garbage Collection Handbook: The Art of Automatic Memory Management. CRC Applied Algorithms and Data Structures Series; Chapman and Hall / CRC Press / Taylor & Francis Ltd., 2011.

[4] Popov, A.S. Cubature formulas on a sphere invariant under the symmetry groups of regular polyhedrons. Siberian Electronic Mathematical Reports 2017, 14, 190–198. doi:10.17377/semi.2017.14.019.

[5] Popov, A.S. Cubature formulas on a sphere invariant under the icosahedral rotation group. Numer. Analys. Appl. 2008, 1, 355–361. doi:10.1134/S199542390804006X.

Yuri A. Blinkov
Saratov State University
Saratov, Russia
e-mail: blinkovua@sgu.ru

Rustam E. Bayramov
Department of Applied Probability and Informatics
Peoples' Friendship University of Russia,
Moscow, Russia

e-mail: 1032212309@rudn.ru

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

e-mail: malykh_md@pfur.ru

Multifrequency resonant conditions in Hamiltonian systems

Alexander Bruno, Alexander Batkhin and Zafar Khaydarov

Abstract. The conditions on the coefficients of the characteristic polynomial of the matrix of the linearized Hamiltonian system, under which this polynomial has roots satisfying the resonance equation, are formulated. These conditions are described as roots of quasi-homogeneous polynomials defined in the coefficient space.

Introduction

Resonances play an essential role in vibrational systems. Their presence, on the one hand, leads to complex dynamics, when the energy of vibrations is "pumped" between several degrees of freedom, whose corresponding frequencies are in resonance. On the other hand, the presence of nontrivial solutions of the resonance equation allows to write additional formal first integrals and, as a consequence, allows to analyze the stability of the equilibrium position or to integrate asymptotically the system of equations of motion reduced to the normal form.

Consider an analytic Hamiltonian system

$$\dot{\mathbf{x}} = \frac{\partial H}{\partial \mathbf{y}}, \quad \dot{\mathbf{y}} = -\frac{\partial H}{\partial \mathbf{x}} \tag{1}$$

with n degrees of freedom, where $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, near the equilibrium position

$$\mathbf{x} = \mathbf{y} = 0.$$

The Hamilton function $H(\mathbf{x}, \mathbf{y})$ expands into a convergent power series

$$H(\mathbf{x}, \mathbf{y}) = \sum H_{\mathbf{pq}} \mathbf{x}^{\mathbf{p}} \mathbf{y}^{\mathbf{q}}$$

with constant coefficients $H_{\mathbf{pq}}$, where $\mathbf{p}, \mathbf{q} \geq 0$, $|\mathbf{p}| + |\mathbf{q}| \geq 2$.

Introduce a phase vector $\mathbf{z} = (\mathbf{x}, \mathbf{y}) \in \mathbb{R}^{2n}(\mathbb{C}^{2n})$. Then the linear part of the system (1) can be written in the form

$$\dot{\mathbf{z}} = B\mathbf{z}, \quad B = \frac{1}{2}\begin{pmatrix} \dfrac{\partial^2 H}{\partial \mathbf{y}\partial \mathbf{x}} & \dfrac{\partial^2 H}{\partial \mathbf{y}\partial \mathbf{y}} \\ -\dfrac{\partial^2 H}{\partial \mathbf{x}\partial \mathbf{x}} & -\dfrac{\partial^2 H}{\partial \mathbf{x}\partial \mathbf{y}} \end{pmatrix}\Bigg|_{\mathbf{x}=\mathbf{y}=0} \tag{2}$$

Let $\lambda_1, \ldots, \lambda_{2n}$ be the eigenvalues of matrix B, which can be reordered as follows $\lambda_{j+n} = -\lambda_j$, $j = 1, \ldots, n$. Denote by vector $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_n)$ the set of basic eigenvalues of the system (2). For a Hamiltonian system, the characteristic polynomial $\check{f}(\lambda)$ is the polynomial of even powers of λ. Let us call the polynomial $f(\mu) \stackrel{\text{def}}{=} \check{f}(\lambda)$, where $\mu = \lambda^2$, as *semi-characteristic*:

$$f(\mu) = \mu^n + a_1\mu^{n-1} + a_2\mu^{n-2} + \cdots + a_{n-1}\mu + a_n. \tag{3}$$

According to Theorem 12 in [1, § 12] in the case of semi-simple eigenvalues there exists a canonical formal transformation that reduces the Hamiltonian system (1) to its *normal form*

$$\dot{\mathbf{u}} = \partial h/\partial \mathbf{v}, \quad \dot{\mathbf{v}} = -\partial h/\partial \mathbf{u},$$

given by the normalized Hamiltonian $h(\mathbf{u}, \mathbf{v})$

$$h(\mathbf{u}, \mathbf{v}) = \sum_{j=1}^{n} \lambda_j u_j v_j + \sum h_{\mathbf{pq}}\mathbf{u}^{\mathbf{p}}\mathbf{v}^{\mathbf{q}} \tag{4}$$

containing only the resonant terms $h_{\mathbf{pq}}\mathbf{u}^{\mathbf{p}}\mathbf{v}^{\mathbf{q}}$ satisfying the *resonant equation*

$$\langle \mathbf{p} - \mathbf{q}, \boldsymbol{\lambda} \rangle = 0. \tag{5}$$

Here $\langle \mathbf{p}, \boldsymbol{\lambda} \rangle = \sum\limits_{j} = 1^n p_j\lambda_j$ is the scalar product.

The resonant equation (5) has two kinds of solutions, which correspond to two kinds of resonant terms in the normal form (4):

1. *Secular terms* of the form $h_{\mathbf{pp}}\mathbf{u}^{\mathbf{p}}\mathbf{v}^{\mathbf{p}}$, which are always present in the Hamiltonian normal form because of the special structure of the matrix B of the linearized system (2)
2. *Strictly resonant terms*, which correspond to nontrivial integer solutions of the equation

$$\langle \mathbf{p}, \boldsymbol{\lambda} \rangle = 0. \tag{6}$$

To investigate the formal stability of the equilibrium position of the Hamiltonian system it is necessary to perform a normalization procedure and then apply Bruno's theorem [3], the condition of which requires the absence of third- and fourth-order resonances. The conditions on the coefficients of the polynomial (3) for two-frequency resonances are effectively formulated in terms of q-discriminants [4].

The problem is the following: formulate conditions on the coefficients a_j, $j = 1, \ldots, n$, of the semi-characteristic polynomial $f(\mu)$ of degree $n = 3$ and

$n = 4$, under which the multifrequency resonance of multiplicity 1 of order 3 or order 4 takes place.

1. Conditions for a system with three degrees of freedom

The only multifrequency resonance of multiplicity 1 of order 3 corresponds to the case where the algebraic sum of all three basic eigenvalues λ_j, $j = 1, 2, 3$, is equal to zero. Then in terms of roots μ_j of the polynomial (3) this condition is written as

$$\mu_1 = A \pm 2C, \text{ where } A = \mu_2 + \mu_3, C^2 = \mu_2\mu_3. \tag{7}$$

Considering the condition (7) as a polynomial ideal, we compute the Gröbner elimination basis that excludes the quantities A and C, and obtain the condition on roots:

$$\sum_{j=1}^{3} \mu_j^2 - 2 \sum_{1=j<k}^{3} \mu_j \mu_k = \sigma_1^2(\mu) - 4\sigma_2(\mu), \tag{8}$$

where $\sigma_k(\mu)$ are elementary symmetric polynomials for which $\sigma_k(\mu) = (-1)^k a_k$. Then the condition on the coefficients of the polynomial (3) takes the form

$$a_1^2 - 4a_2 = 0. \tag{9}$$

The condition for the existence of multifrequency resonance of multiplicity 1 of order 4 is equivalent to the case of the algebraic sum of $2\lambda_1$, λ_2, λ_3 equals to zero. Repeating the above calculations, we get a condition on the coefficients of the polynomial (3) in the form

$$16\, a_1^6 - 264\, a_1^4 a_2 + 36\, a_1^3 a_3 + 1425\, a_1^2 a_2^2 - 630\, a_1 a_2 a_3 - 2500\, a_2^3 + 9261\, a_3^2 = 0. \tag{10}$$

The conditions (9) and (10) are algebraic varieties in the coefficient space of the polynomial (3) for $n = 3$, and their left-hand sides are quasi-homogeneous polynomials from coefficients a_j, $j = 1, 2, 3$. By methods of power geometry one can obtain a polynomial parametrization of the variety (10):

$$a_1 = 2v\,(37t - 35)\,, a_2 = \left(456337t^2 - 7666t + 721\right) v^2,$$
$$a_3 = 36\,(71t + 2)\,(5 - 249t)^2\, v^3.$$

Note that many works on oscillation theory consider multifrequency resonances of multiplicities 2 and higher. For example, a resonance of order 4 in the form of commensurable frequencies 2 : 1 : 1 has multiplicity 2 and is defined using the conditions on two-frequency resonances. The 1 : 1 commensurability is determined by the discriminant variety $\mathcal{D}(f)$ of dimension 2, the 2 : 1 commensurability is determined by the resonant variety $\mathcal{R}_4(f)$ of dimension 2, and their intersection gives the submanifold of dimension 1 on which the above resonance takes place. At the same time, the condition (10) for the existence of a three-frequency resonance of multiplicity 1 defines a variety of dimension 2, i. e. it is a more general condition.

2. Conditions for a system with four degrees of freedom

In this case, the situations of three-frequency and four-frequency resonances should already be considered separately. We have two three-frequency resonances of orders 3 and 4, and one four-frequency resonance of order 4.

The condition on roots (8) of three-frequency resonance of order 3 for a polynomial of degree 4 must be satisfied for some one triplet of roots μ_k, $k = 1, \ldots, 4$. Then we make a product of four factors of the form (7) for each triplet and add it to the ideal composed of polynomials of the form $a_k - \sigma_k$, $k = 1, \ldots, 4$. Using the Gröbner elimination basis, we exclude the values of μ_k and obtain a condition on the coefficients of the form

$$-4\,a_1^5 a_3 + a_1^4 a_2^2 + 4\,a_1^4 a_4 + 34\,a_1^3 a_2 a_3 - 8\,a_1^2 a_2^3 - 30\,a_1^2 a_2 a_4 - 27\,a_1^2 a_3^2 - 72\,a_1 a_{2^2 a_3} + 16\,a_2^4 - 54\,a_1 a_3 a_4 + 72\,a_2^2 a_4 + 108\,a_2 a_3^2 + 81\,a_4^2 = 0.$$

We can do the same to determine the condition on the roots of the polynomial in the presence of a three-frequency resonance of order 4 for a polynomial of degree 4. The resulting polynomial turns out to be very cumbersome (it contains 153 monomials) and is not given here.

Finally, let us indicate the condition on the coefficients of the polynomial (3) of the fourth order which, if satisfied, leads to a four-frequency resonance of order 4:

$$a_1^4 - 8\,a_1^2 a_2 + 16\,a_2^2 - 64\,a_4 = 0.$$

References

[1] A. D. Bruno. Analytical form of differential equations (II). *Trans. Moscow Math. Soc.*, 26:199–239, 1972. = Trudy Moskov. Mat. Obsc. 25 (1971) 119-262 (in Russian).

[2] A. D. Bruno. *The Restricted 3–body Problem: Plane Periodic Orbits*. Walter de Gruyter, Berlin, 1994. = Nauka, Moscow, 1990. 296 p. (in Russian).

[3] A. D. Bruno. Formal stability of Hamiltonian systems. *Math. Notes*, 1(3):216–219, 1967.

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

Alexander Bruno
Department of Singular Problems
Keldysh Institute of Applied Mathematics of RAS
Moscow, Russia
e-mail: abruno@keldysh.ru

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

Zafar Khaydarov
Mechanics and Mathematics Dept.
Samarkand State University named after Sh. Rashidov
Samarkand, Uzbekistan
e-mail: zafarxx@gmail.com

On basic stratified structures in quantum information geometry

M.Bureš, A.Khvedelidze, D.Mladenov and S.Velkov

Searching for non-trivial physical consequences of quantum theory, the knowledge of the mathematical structure of the set of quantum states can be a reliable guide. The state space $\mathfrak{P}_N$ of an N-level quantum system consists of $N \times N$ Hermitian, normalized semi-positive density matrices,

$$\mathfrak{P}_N = \{ X \in M_N(\mathbb{C}) \,|\, X = X^\dagger ,\ X \geq 0 ,\ \mathrm{Tr}\, X = 1 \} .$$

During the last two decades, following the request coming from the advanced quantum technologies and quantum information science, the state space $\mathfrak{P}_N$ has been studied in various contexts, among them convex-geometric, topological, differential-geometric, etc. (see, e.g. reviews [1, 2, 3] and references therein.)

In the present report, we discuss some features of the underlying stratified structure of $\mathfrak{P}_N$. It will be outlined that among three admissible partitions of $\mathfrak{P}_N$, namely by the adjoint $SU(N)$ orbits, by the corresponding orbit types, or by the subsets of density matrices with fixed ranks, only the last decomposition determines the Whitney stratification. Based on this observation, we expand some results of our recent paper [4], devoted to the study of the Bures-Fisher metric for rank deficient states, which are non-maximal dimensional strata of the Whitney stratification. We comment on the existence of a generalized stratified metric on the whole state space.

The first author was supported from EU Regional Development Fund-Project No.CZ.02.1.01/0.0/0.0/16_019/0000766. The research of A.K and D.M was supported in part by the Collaborative grant "Bulgaria-JINR".

References

[1] I. Bengtsson and K. Zyczkowski, Geometry of Quantum States: An Introduction to Quantum Entanglement, 2nd edition. Cambridge University Press, (2017)

[2] S. Amari, Information Geometry and Its Applications, Springer, Japan, 2016.

[3] F. D'Andrea and D. Franco, On the pseudo-manifold of quantum states, Differential Geometry and its Applications 78, 101800 (2021).

[4] M. Bures, A. Khvedelidze and D. Mladenov, Solving the Uhlmann Equation for the Bures-Fisher Metric on the Subset of Rank-Deficient Qudit States, 9th International Conference on Distributed Computing and Grid Technologies in Science and Education, 358-362 (2021).

M.Bureš
Institute of Experimental and Applied Physics
Czech Technical University in Prague
Husova 240/5, 110 00 Prague 1, Czech Republic
&
Laboratory of Information Technologies
Joint Institute for Nuclear Research
141980 Dubna, Russia
e-mail: bures@physics.muni.cz

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

D.Mladenov
Theoretical Physics Department, Faculty of Physics
Sofia University "St Kliment Ohridski"
5 James Bourchier Blvd,
1164 Sofia, Bulgaria
e-mail: dimitar.mladenov@phys.uni-sofia.bg

S.Velkov
Theoretical Physics Department, Faculty of Physics
Sofia University "St Kliment Ohridski"
5 James Bourchier Blvd,
1164 Sofia, Bulgaria
e-mail: stanislavbg@yahoo.co.uk

On the Integrability of the Polynomial Case of a Liénard-type Equation

Victor F. Edneral

Abstract. The paper investigates the connection between the global integrability of an autonomous two-dimensional polynomial ODE system and its local integrability near stationary points using the example of the polynomial case of a Lenar-type equation. We presented the equation in the form of a dynamical system and parametrized it. The conditions for local integrability near stationary points are written out and the values of the parameters under which these conditions are satisfied are found. It is established that for certain values of the parameters obtained in this way, the system actually turns out to be integrable. Thus, we can speak of a heuristic approach that allows one to determine the cases of ODE integrability.

Introduction

We use an approach based on local analysis. It uses the resonant normal form computed near stationary points [1]. In [2], a method was proposed for finding parameter values for which the dynamical system is locally integrable at all stationary points simultaneously. The main idea is that in the domain of integrability in the phase space, a necessary condition is local integrability at every point of this domain. But at regular points, local integrability already takes place, so local integrability is also necessary at singular points, and at all such points of the domain under consideration.

Note that for the global integrability of an autonomous planar system, it suffices to have one global integral of motion. From its expression, one can obtain a solution of the system in quadratures; therefore, integrability implies the solvability of the system.

This paper has been supported by the RUDN University Strategic Academic Leadership Program (recipient A.A., mathematical model development).

Problem

We will check our method on the example of the Liénard-like equation

$$\ddot{x} = f(x)\dot{x} + g(x), \tag{1}$$

Here we assume that $f(x)$ and $g(x)$ are polynomials. Usually, the Linard equation assumes that $f(x)$ is an even function and $g(x)$ is an odd function [3] . We do not assume a certain parity for them, so we are talking about the Linard-type equation.

Equation (1) is equivalent to the dynamical system

$$\begin{aligned} \dot{x} &= y, \\ \dot{y} &= (a_0 + a_1 x)\, y + b_1 x + b_2 x^2 + b_3 x^3, \end{aligned} \tag{2}$$

here x and y are functions in time and parameters a_0, a_1, b_1, b_2, b_3 are real.

The problem is to construct the first integrals of system (2).

Method

Note that for the global integrability of an autonomous planar system, it suffices to have one global integral of motion. From its expression, one can obtain a solution of the system in quadratures; therefore, integrability implies the solvability of the system. The main task of the method under discussion is to find conditions on the parameters of the system under which the system is locally integrable near its stationary points. Local integrability means the presence of a sufficient number (one for an autonomous flat system) of local integrals at each point of the region under study, including the corresponding stationary points. Local integrals may be different for each point of this region of the phase space, but for the existence of a global integral, local integrals must exist for the desired values of the parameters at all fixed points. This is a necessary condition. In papers [1] the algebraic condition of local integrability is written out. This is the so-called **A** condition. This condition is satisfied at all regular points, but it is nontrivial at stationary points.

First, we look for sets of parameters under which the condition **A** is satisfied at the fixed point of the system at the origin (2). We solve the corresponding systems of algebraic equations with respect to the parameters a_0, a_1, b_1, b_2, b_3 and check the integrability at other stationary points for each found set of parameters. "Good" sets of parameters are good candidates for the existence of a single function for all points - the first integral. These integrals are sought by the method described below.

Conditions of the Integrability

The condition **A** is some infinite sequence of polynomial equations with respect to the coefficients of the system. Each of the stationary points has its own system of equations. But the normal form has a non-trivial form only in the resonant case.

This means that we can only use our method if the eigenvalues of the linear part of the system (2) refer as integers. We restrict our study to this case for now. A possible condition for these eigenvalues to be related as $1 : M$ and have opposite signs (the resonance case) is the relation

$$a_0 - \sqrt{a_0^2 + 4b_1} = -M\left(a_0 + \sqrt{a_0^2 + 4b_1}\right).$$

We choose the "resonance" restriction on parameters in the form

$$b_1 = \frac{a_0^2 M}{(M-1)^2}. \tag{3}$$

From the A condition, we constructed three equations for the system parameters a_0, a_1, b_2, b_3 for the $(1:2), (1:3)$ and $(1:4)$ resonances, i.e. for $M = 2, 3, 4$. Here is the first of three equations for $M = 2$ as an example

$$a_0{}^3\left(2a_1{}^3 - 29a_1b_3\right) + a_0{}^2 b_2\left(26a_1{}^2 + 43b_3\right) + 13a_0a_1b_2{}^2 - 11b_2{}^3 = 0.$$

Results

For the case with resonance $M = 2$ the solutions of the corresponding algebraic system calculated by the MATHEMATICA-11 system are

$$\begin{array}{ll} 1) & \{a_0 \to 0, b_2 \to 0\}, \\ 2) & \{b_2 \to -a_0a_1, b_3 \to 0\}, \\ 3) & \{b_2 \to -4a_0a_1/7, b_3 \to -6/49\, a_1{}^2\}, \\ 4) & \{b_2 \to -a_0a_1/3, b_3 \to -a_1{}^2/9\}, \\ 5) & \{b_2 \to 3a_0a_1, b_3 \to a_1{}^2\}, \\ 6) & \{a_1 \to 0, b_2 \to 0, b_3 \to 0\}. \end{array} \tag{4}$$

Here $b_1 \to 2a_0^2$ for $M = 2$. At these sets of parameters we checked the integrability condition at other stationary points of (2).

The autonomous system of the second order(2) can be rewrite as the first order non-autunomous equation

$$\begin{array}{l} dy(x)/dx = [(a_0 + a_1x)\, y(x) + b_1x + b_2x^2 + b_3x^3]/y(x) \\ \quad \text{or} \\ dx(y)/dy = x(y)/[(a_0 + a_1x(y))\, y + b_1x(y) + b_2x(y)^2 + b_3x(y)^3]. \end{array} \tag{5}$$

After this rewrite, we tried to solve such equations with each of the parameter sets (4) using the MATHEMATIC-11 solver. We have found solutions for sets 2), 4), 5) and 6) in the implicit form of $F(y(x), x, C) = 0$. We then expressed the constant C as a function in $x, y(x)$ and replaced these variables with $x(t)$ and $y(t)$. Thus, we obtain integrals of motion. The resulting integrals can be verified by direct calculation of the time derivative along the system.

The integrable cases in (4) correspond to the equations

$$\begin{array}{ll} 2) & \ddot{x} = (a_0 + a_1 x)\,\dot{x} + 2{a_0}^2 x - a_0 a_1 x^2, \\ 4) & \ddot{x} = (a_0 + a_1 x)\,\dot{x} + 2{a_0}^2 x - \frac{1}{3} a_0 a_1 x^2 - \frac{1}{9}{a_1}^2 x^3, \\ 5) & \ddot{x} = (a_0 + a_1 x)\,\dot{x} + 2{a_0}^2 x + 3 a_0 a_1 x^2 + {a_1}^2 x^3. \end{array} \qquad (6)$$

We returned here from the systems of equations to the equations of the second order. For equation 2) the first integral is

$$\frac{(a_1 x(t) - 2a_0)\sinh\left(\frac{1}{2}R(x(t),y(t))\right) + a_0 R(x(t),y(t))\cosh\left(\frac{1}{2}R(x(t),y(t))\right)}{(a_1 x(t) - 2a_0)\cosh\left(\frac{1}{2}R(x(t),y(t))\right) + a_0 R(x(t),y(t))\sinh\left(\frac{1}{2}R(x(t),y(t))\right)},$$

where

$$R(x(t),y(t)) = \sqrt{\frac{a_1(x(t)(a_1 x(t) - 2a_0) - 2y(t))}{{a_0}^2}}.$$

We have done the above steps for $M = 2, 3$ resonances with the same results. The coefficient b_1 for x in (6) is fixed everywhere, since $b_1 = 2a_0^2$ for $M = 2$, but for other M it will be different.

Note also that case 4) in (6) (6) is exactly a special case of equation 4 from section 2.2.3-2 of [4] with parameters $a_0 \to b, a_1 \to 3a, c \to 2b^2$. But the fact that cases 2) and 5) are integrable is a new result, at least for this book.

References

[1] A.D. Bruno, *Analytical form of differential equations (I, II)*. Trudy Moskov. Mat. Obsc. **25**, 119–262 (1971), **26**, 199–239 (1972) (in Russian) = Trans. Moscow Math. Soc. **25**, 131–288 (1971), **26**, 199–239 (1972) (in English) A.D. Bruno, *Local Methods in Nonlinear Differential Equations.* Nauka, Moscow 1979 (in Russian) = Springer-Verlag, Berlin (1989) P.348.

[2] A.D. Bruno, V.F. Edneral, V.G. Romanovski, On new integrals of the Algaba-Gamero-Garcia system, Proceedings of the CASC 2017, Springer-Verlag series: LNCS **10490** (2017) 40–50

[3] A. Liénard, Etude des oscillations entretenues, Revue générale de l'électricité **23** (1928) 901–912 and 946–954.

[4] A.D. Polyanin, V.F. Zaitsev, *Handbook of exact solutions for ordinary differential equations–2nd ed.* Chapman & Hall/CRC Press (2003) P. 803.

Victor F. Edneral
Skobeltsyn Institute of Nuclear Physics of Lomonosov Moscow State University
1(2) Leninskie gory, Moscow, 119991, Russian Federation
and
Peoples' Friendship University of Russia (RUDN University)
6 Miklukho-Maklaya St, Moscow, 117198, Russian Federation
e-mail: edneral@theory.sinp.msu.ru; edneral-vf@rudn.ru

Around concurrent normal conjecture

Alexandr Grebennikov and Gaiane Panina

Given a smooth convex body $K \in \mathbb{R}^n$, its normal to a point $p \in \partial K$ is a line passing through p and orthogonal to ∂K at the point p. It is conjectured that for any convex body $K \in \mathbb{R}^n$ there exists a point in the interior of K which is the intersection point of at least $2n$ normals from different points on the boundary of K. The concurrent normals conjecture trivially holds for $n = 2$. For $n = 3$ it was proven by Heil via geometrical methods and reproved by Pardon via topological methods. The case $n = 4$ was completed also by Pardon.

Recently Martinez-Maure proved for $n = 3, 4$ that (under mild conditions) almost every normal through a boundary point to a smooth convex body K passes arbitrarily close to the set of points lying on normals through at least six distinct points of ∂K. He used Minkowski differences of smooth convex bodies, that is, the *theory of hedgehogs*.

We give a very short proof of a slightly more general result: *for dimension* $n \geq 3$, *under mild conditions, almost every normal through a boundary point to a smooth convex body* $K \in \mathbb{R}^n$ *contains an intersection point of at least* 6 *normals from different points on the boundary of* K.

Our proof is based on the bifurcation theory and does not use hedgehogs.

Acknowledgments. G. Panina is supported by RFBR grant 20-01-00070A; A. Grebennikov is supported by Ministry of Science and Higher Education of the Russian Federation, agreement 075-15-2019-1619.

Alexandr Grebennikov
Department of Mathematics and Computer Sciences
Saint-Petersburg State University
Saint-Petersburg, Russia
e-mail: `sagresash@yandex.ru`

Gaiane Panina
Dept. name of organization
Saint-Petersburg Department of Steklov Mathematical Institute
Saint-Petersburg, Russia
e-mail: `gaiane-panina@rambler.ru`

Algebraic solution of a scheduling problem in project management

Gubanov S. A., Design bureau "Luch", software engineer,
segubanov@mail.ru

Abstract. A project scheduling problem is examined, where the maximum deviation of start time of jobs is minimized under various constraints imposed on the start and finish time of jobs. We represent the problem in terms of tropical algebra as a tropical optimization problem, and then obtain a direct solution given in compact vector form.

1. Introduction

One of the main problems of the project management is the problem of drawing up an optimal schedule of jobs in a project [1, 2]. To solve scheduling problems, models and methods of tropical mathematics are used, which studies semirings and semifields with idempotent addition [3, 4, 5]. Scheduling problems are reduced to optimization problems formulated and solved in terms of tropical mathematics (tropical optimization problems) [6, 7, 8, 9]. In this paper we consider the problem of minimizing the maximum deviation of the start times of jobs from the due dates under given various temporal constraints. The problem is represented as a tropical optimization problem, and then solved using a result of the paper [10].

2. Optimal scheduling problem

We consider a problem which arises in project management where an optimal schedule for a project is developed to minimize the maximum deviation of start times of jobs from given due dates.

Let us consider a project which consists of n jobs performed in parallel, subject to time constraints in the form of “start-start”, “start-finish”, and “finish-start” precedence relationships, as well as boundaries for the start and finish times of jobs.

2 Gubanov S. A., Design bureau "Luch", software engineer, segubanov@mail.ru

For each job $i = 1, \dots, n$, we denote the start time by x_i and the finish time by y_i. Let the values g_i and h_i define the earliest and latest allowed start time, as well as f_i defines the latest finish time. These values set boundaries for the start and finish times in the form of the inequalities

$$g_i \leq x_i \leq h_i, \qquad y_i \leq f_i.$$

The "start-start" constraints for the job i are defined in the form of inequalities $b_{ij} + x_j \leq x_i$ for all $j = 1, \dots, n$, where b_{ij} denotes the minimum allowed time interval between the start of job i and the start of j. We put $b_{ij} = -\infty$ if the value b_{ij} is not set. Combining the inequalities over all j gives the equivalent inequality

$$\max_{1 \leq j \leq n} (b_{ij} + x_j) \leq x_i.$$

Let us denote the minimum allowed interval between the start time of i and the finish time of j by c_{ij} ($c_{ij} = -\infty$ if the interval is not specified) and write the "start-finish" constraint in the form of the inequality $c_{ij} + x_j \leq y_i$. We assume that the job finishes immediately when the "start-finish" constraints are satisfied, and then the equality $c_{ij} + x_j = y_i$ is satisfied for at least one j. After combining the inequalities for all j, we obtain

$$\max_{1 \leq j \leq n} (c_{ij} + x_j) = y_i.$$

We denote the minimum allowed interval between the finish time of job i and the start time of j by d_{ij} ($d_{ij} = -\infty$ if no interval is specified). The "finish-start" constraints are written as the inequalities $d_{ij} + y_j \leq x_i$, which are combined into the inequality

$$\max_{1 \leq j \leq n} (d_{ij} + y_j) \leq x_i.$$

Suppose that for each job i, a due date p_i is given, which determines the most desirable start time. We formulate a problem of minimizing the maximum deviation of start time of jobs from the due dates under given constraints as the problem of determining for all $i = 1, \dots, n$ the values x_i and y_i to find

$$\begin{aligned} \min_{x_i, y_i} \quad & \max\left(\max_{1 \leq i \leq n} (p_i - x_i), \max_{1 \leq i \leq n} (x_i - p_i) \right); \\ & \max_{1 \leq j \leq n} (b_{ij} + x_j) \leq x_i, \quad \max_{1 \leq j \leq n} (c_{ij} + x_j) = y_i, \\ & \max_{1 \leq j \leq n} (d_{ij} + y_j) \leq x_i, \quad g_i \leq x_i \leq h_i, \\ & y_i \leq f_i, \quad i = 1, \dots, n. \end{aligned} \tag{1}$$

Below, this problem is formulated in terms of tropical mathematics and solved by using methods of tropical optimization.

3. Elements of tropical mathematics

Let us outline the main definitions and results of tropical (idempotent) mathematics [7, 8, 4, 5], which are used in the next section for describing and solving tropical optimization problems.

Let $\mathbb{X}$ be a set that is closed under the associative and commutative operations of addition $\oplus$ and multiplication $\otimes$, and contain their neutral elements zero $\mathbb{0}$ and one $\mathbb{1}$. Addition is idempotent (for each $x \in \mathbb{X}$ the equality $x \oplus x = x$ holds), while multiplication is distributive with respect to addition and invertible (for any $x \neq \mathbb{0}$ there exists x^{-1} such that $x \otimes x^{-1} = \mathbb{1}$). The algebraic system $\langle \mathbb{X}, \mathbb{0}, \mathbb{1}, \oplus, \otimes \rangle$ is called an idempotent semifield. The sign $\otimes$ of the multiplication operation will be omitted from now on.

Idempotent addition defines a partial order: $x \leq y$ if and only if $x \oplus y = y$. We assume that this partial order extends to a linear order on $\mathbb{X}$.

For any $x \neq \mathbb{0}$ and integer $p > 0$, an integer power is defined in the usual way: $x^0 = \mathbb{1}$, $x^p = x^{p-1}x$, $x^{-p} = (x^{-1})^p$, $\mathbb{0}^p = \mathbb{0}$. It is assumed that the powers with rational exponents are also defined.

An example of the idempotent semifield is the real semifield $\mathbb{R}_{\max,+} = \langle \mathbb{R} \cup \{-\infty\}, -\infty, 0, \max, + \rangle$ for which $\mathbb{0} = -\infty$, $\mathbb{1} = 0$, $\oplus = \max$ and $\otimes = +$.

Let us denote by $\mathbb{X}^{m \times n}$ the set of matrices which consist of m rows and n columns with elements from $\mathbb{X}$. Addition and multiplication of conforming matrices $\boldsymbol{A} = (a_{ij})$, $\boldsymbol{B} = (b_{ij})$ and $\boldsymbol{C} = (c_{ij})$, as well as multiplication by a scalar x are defined by the formulas

$$\{\boldsymbol{A} \oplus \boldsymbol{B}\}_{ij} = a_{ij} \oplus b_{ij}, \quad \{\boldsymbol{B}\boldsymbol{C}\}_{ij} = \bigoplus_{k} b_{ik} c_{kj}, \quad \{x\boldsymbol{A}\}_{ij} = x a_{ij}.$$

The order relation given above is extended to matrices and is understood entrywise.

Consider square matrices in $\mathbb{X}^{n \times n}$. The matrix $\boldsymbol{I}$ with elements equal to $\mathbb{1}$ on the main diagonal and $\mathbb{0}$ outside it is the identity matrix.

For any square matrix $\boldsymbol{A} = (a_{ij})$ and integer $p > 0$ the power is given by: $\boldsymbol{A}^0 = \boldsymbol{I}$, $\boldsymbol{A}^p = \boldsymbol{A}^{p-1}\boldsymbol{A}$. We define the functions

$$\operatorname{tr} \boldsymbol{A} = \bigoplus_{i=1}^{n} a_{ii}, \quad \operatorname{Tr}(\boldsymbol{A}) = \bigoplus_{k=1}^{n} \operatorname{tr} \boldsymbol{A}^k,$$

If $\operatorname{Tr}(\boldsymbol{A}) \leq \mathbb{1}$, then the Kleene matrix is defined in the form

$$\boldsymbol{A}^* = \bigoplus_{k=0}^{n-1} \boldsymbol{A}^k.$$

The set of column vectors consisting of n elements is denoted by $\mathbb{X}^n$.

A vector without zero elements is called regular.

4 Gubanov S. A., Design bureau "Luch", software engineer, segubanov@mail.ru

For any nonzero vector $\boldsymbol{x} = (x_i) \in \mathbb{X}^n$, the transposed vector is denoted as $\boldsymbol{x}^T$. The multiplicatively conjugate vector for $\boldsymbol{x}$ is the row vector $\boldsymbol{x}^- = (x_i^-)$, where $x_i^- = x_i^{-1}$ if $x_i \neq \mathbb{0}$ and $x_i^- = \mathbb{0}$ – otherwise.

4. Solution of the optimal planning problem

Let us formulate the problem (1) in terms of the idempotent semifield $\mathbb{R}_{\max,+}$. We denote the following matrices and vectors:

$$\boldsymbol{B} = (b_{ij}), \quad \boldsymbol{C} = (c_{ij}), \quad \boldsymbol{D} = (d_{ij}),$$
$$\boldsymbol{x} = (x_i), \quad \boldsymbol{y} = (y_i), \quad \boldsymbol{f} = (f_i), \quad \boldsymbol{g} = (g_i), \quad \boldsymbol{h} = (h_i), \quad \boldsymbol{p} = (p_i).$$

The problem (1) in vector notation has the form

$$\begin{aligned} \min_{\boldsymbol{x},\boldsymbol{y}} \quad & \boldsymbol{x}^-\boldsymbol{p} \oplus \boldsymbol{p}^-\boldsymbol{x}, \\ & \boldsymbol{B}\boldsymbol{x} \leq \boldsymbol{x}, \quad \boldsymbol{C}\boldsymbol{x} = \boldsymbol{y}, \quad \boldsymbol{D}\boldsymbol{y} \leq \boldsymbol{x}, \quad \boldsymbol{g} \leq \boldsymbol{x} \leq \boldsymbol{h}, \quad \boldsymbol{y} \leq \boldsymbol{f} \end{aligned} \tag{2}$$

The solution of the problem is described by the following statement.

Lemma 1. *Let $\boldsymbol{B}$ and $\boldsymbol{D}$ be matrices, $\boldsymbol{C}$ be a column-regular matrix such that the matrix $\boldsymbol{R} = \boldsymbol{B} \oplus \boldsymbol{D}\boldsymbol{C}$ satisfies $\mathrm{Tr}(\boldsymbol{R}) \leq \mathbb{1}$. Let $\boldsymbol{g}$ be a vector, and $\boldsymbol{f}$ and $\boldsymbol{h}$ be regular vectors such that the vector $\boldsymbol{s}^T = \boldsymbol{f}^-\boldsymbol{C} \oplus \boldsymbol{h}^-$ satisfies the condition $\boldsymbol{s}^T\boldsymbol{R}^*\boldsymbol{g} \leq \mathbb{1}$.*

Then the minimum value of the objective function in problem (2) is equal to

$$\theta = (\boldsymbol{p}^-\boldsymbol{R}^*\boldsymbol{p})^{1/2} \oplus \boldsymbol{s}^T\boldsymbol{R}^*\boldsymbol{p} \oplus \boldsymbol{p}^-\boldsymbol{R}^*\boldsymbol{g},$$

and all regular solutions have the form

$$\boldsymbol{x} = \boldsymbol{R}^*\boldsymbol{u}, \quad \boldsymbol{y} = \boldsymbol{C}\boldsymbol{R}^*\boldsymbol{u}, \tag{3}$$

where $\boldsymbol{u}$ is any regular vector which satisfies the conditions

$$\boldsymbol{g} \oplus \theta^{-1}\boldsymbol{p} \leq \boldsymbol{u} \leq ((\boldsymbol{s}^T \oplus \theta^{-1}\boldsymbol{p}^-)\boldsymbol{R}^*)^-. \tag{4}$$

5. Conclusion

A project scheduling problem is considered, which consists in minimizing the maximum deviation of start times of jobs from given due dates under given constraints of the form “start-start”, “start-finish”, “finish-start” and boundaries for the earliest and latest allowed start time. A direct solution of the problem is obtained, which can be used for both formal analysis and direct calculations.

References

[1] T'kindt V. and Billaut J.-C. , Multicriteria Scheduling. 2 ed. Berlin: Springer, 2006.

[2] *Kerzner H.* Project Management. 10 ed. Hoboken: Wiley, 2010. 1094 p.

[3] Maslov V. P., Kolokoltsev V. N. Idempotent analysis and its application in optimal control. Moscow: Fizmatlit, 1994.

[4] Methods of Idempotent Algebra in Problems of Complex Systems Modeling and Analysis St. Petersburg University Press, St. Petersburg, 2009. 255 p. (in Russian)

[5] Butkovič P., Max-linear Systems: Theory and Algorithms. Springer Monographs in Mathematics. London: Springer, 2010.

[6] Krivulin N. Direct solution to constrained tropical optimization problems with application to project scheduling //Computational Management Science. 2017. Vol. 14. N 1. P. 91-113.

[7] Krivulin N., Tropical optimization problems with application to project scheduling with minimum makespan // Annals of Operations Research. 2017. Vol. 256, N 1. P. 75-92.

[8] Krivulin N., Tropical optimization problems in time-constrained project scheduling. // Optimization. 2017. Vol. 66, N 2. P. 205-224.

[9] Krivulin N. K., Gubanov S. A. Algebraic solution of the problem of assigning a project planning term in project management // Bulletin of St. Petersburg University. Mathematics. Mechanics. Astronomy. 2021. Vol. 8.N 1. P. 73-87.

[10] Krivulin N. Complete solution of a constrained tropical optimization problem with application to location analysis // Relational and Algebraic Methods in Computer Science. Cham: Springer, 2014. P. 362-378. (Lecture Notes in Computer Science, Vol. 8428.)

Gubanov S. A., Design bureau "Luch", software engineer, segubanov@mail.ru

Riemann Hypothesis Property for The Convergents of a Continued Fraction Expansion

Nikita Gogin and Mika Hirvensalo

Abstract. We show that the denominators and numerators of convergents to a continued fraction both satisfy a Riemann Hypothesis property, meaning that their zeros lie in a perpendicular line in a complex plane.

1. Continued fraction representation

We study the function

$$\mathfrak{D}(w) = -w + \cfrac{1^2}{-w + \cfrac{2^2}{-w + \cfrac{3^2}{-w + \cfrac{4^2}{-w + \ddots}}}} = -w + \mathbf{K}_{r=1}^{\infty}\left(\frac{r^2}{-w}\right) \tag{1}$$

first formally, without verifying any convergence property. As usual, the finite initial segments $\mathfrak{D}_m(w)$ of (1) are called *convergents* ([5], [4]). For example, the first convergents are

$$\mathfrak{D}_0(w) = -w, \quad \mathfrak{D}_1(w) = -w + \frac{1}{-w} = \frac{w^2+1}{-w}, \quad \mathfrak{D}_2(w) = -w + \cfrac{1}{-w + \cfrac{4}{-w}} = \frac{-w^3-5w}{w^2+4}.$$

It is plain to see that each $\mathfrak{D}_n(w)$ is a rational, and denoting

$$\mathfrak{D}_n(w) = \frac{P_n(w)}{Q_n(w)}$$

the theory of continued fractions provides ([5], [4]) the recurrence relations

$$P_n(w) = -wP_{n-1}(w) + n^2 P_{n-2} \quad \text{and} \quad Q_n(w) = -wQ_{n-1}(w) + n^2 Q_{n-2}, \tag{2}$$

and the initial conditions $P_0(w) = -w$, $Q_0(1) = 1$, $P_1(w) = w^2 + 1$, $Q_1(w) = -w$ can be read from the representations of the first convergents. It is also customary to define $P_{-1}(w) = 1$ and $Q_{-1}(w) = 0$ to make the recursions (2) valid already for $n \geq 1$. By initial conditions and recursions (2) it is obvious that both $P_n(w)$ and $Q_n(w)$ are in $\mathbb{Z}[w]$ for each $n \geq 0$.

2. Determinant formulas

Lemma 1. *Let notations be as above and*

$$\hat{P}_n(w) = \begin{vmatrix} -w & 1 & 0 & 0 & \cdots & 0 & 0 \\ -3 & -w & 2 & 0 & \cdots & 0 & 0 \\ 0 & -4 & -w & 3 & \cdots & 0 & 0 \\ 0 & 0 & -5 & -w & \ddots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & n-1 & 0 \\ 0 & 0 & 0 & \cdots & -(n+1) & -w & n \\ 0 & 0 & 0 & \cdots & & -1 & -w \end{vmatrix} \tag{3}$$

and

$$\hat{Q}_n(w) = \begin{vmatrix} -w & 2 & 0 & 0 & \cdots & 0 \\ -2 & -w & 3 & 0 & \cdots & 0 \\ 0 & -3 & -w & 4 & \cdots & 0 \\ 0 & 0 & -4 & -w & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & n \\ 0 & 0 & 0 & \cdots & -n & -w \end{vmatrix}. \tag{4}$$

Then $\hat{P}_n(w) = P_n(w)$ and $\hat{Q}_n(w) = Q_n(w)$ for all $n \geq 1$. Notice that (3) and (6) are determinants of $(n+1) \times (n+1)$ and $n \times n$-matrices, respectively, and that the last low subdiagonal element of $\hat{P}_n(w)$ is -1 by purpose.

Proof. We prove the claim for $P_n(w)$ first. For the initial values we have $P_0(w) = -w = \det(-w) = \hat{P}_0(w)$ (the determinant of 1×1-matrix), and $P_1(w) = w^2+1 = \begin{vmatrix} -w & 1 \\ -1 & -w \end{vmatrix}$.

The recurrence for $\hat{P}_n(w)$ may not be self-evident, and hence we illustrate it here for the case $n = 4$:

$$\begin{aligned} P_4(w) &= \begin{vmatrix} -w & 1 & 0 & 0 & 0 \\ -3 & -w & 2 & 0 & 0 \\ 0 & -4 & -w & 3 & 0 \\ 0 & 0 & -5 & -w & 4 \\ 0 & 0 & 0 & -1 & -w \end{vmatrix} = \begin{vmatrix} -w & 1 & 0 & 0 & 0 \\ -3 & -w & 2 & 0 & 0 \\ 0 & -4 & -w & 3 & 0 \\ 0 & -0 & -1 & -w & 4 \\ 0 & -0 & -w & -1 & -w \end{vmatrix} \\ &= -w \begin{vmatrix} -w & 1 & 0 & 0 \\ -3 & -w & 2 & 0 \\ 0 & -4 & -w & 3 \\ 0 & 0 & -1 & -w \end{vmatrix} - 4 \begin{vmatrix} -w & 1 & 0 & 0 \\ -3 & -w & 2 & 0 \\ 0 & -4 & -w & 3 \\ 0 & 0 & -w & -1 \end{vmatrix} \\ &= -wP_3(w) - 4 \begin{vmatrix} -w & 1 & 0 & 0 \\ -3 & -w & 2 & 0 \\ 0 & -1 & -w & 3 \\ 0 & -1 & -w & -1 \end{vmatrix} = -wP_3(w) - 4 \begin{vmatrix} -w & 1 & 0 & 0 \\ -3 & -w & 2 & 0 \\ 0 & -1 & -w & 3 \\ 0 & 0 & 0 & -4 \end{vmatrix} \\ &= -wP_3(w) + 4^2 P_2(w) \end{aligned}$$

In the first line, the last column of the determinant is added to the 3rd last column, and then the Laplace expansion along the last column is applied. After this, the last column of the latter 4×4 determinant is added to the 3rd last column, and then the second-last row is added to the last one, with multiplier -1. The latest stage is the Laplace expansion along to the last row.

It is obvious that this procedure generalizes to $\hat{P}_n(w) = -w\hat{P}_{n-1}(w) + n^2\hat{P}_{n-2}(w)$ for each $n > 2$. Now that the initial conditions and the recurrence formula are same for $\hat{P}_n(w)$ and $P_n(w)$, the claim follows.

In the same way, $\hat{Q}_1(w) = -w = Q_1(w)$, $\hat{Q}_2(w) = \begin{vmatrix} -w & 2 \\ -2 & -w \end{vmatrix} = w^2 + 4 = Q_2(w)$. As a determinant of a tridiagonal matrix, $\hat{(Q)}_n(w)$ satisfies the recurrence relation $\hat{Q}_n(w) = -w\hat{Q}_{n-1}(w) + n^2\hat{Q}_{n-2}(w)$. □

Remark 1. *The numerator sequence $P_n(w)$ is equal, up to constant multipliers, to Kratwchouk polynomials ([3]). On the other hand, the denominator sequence $Q_n(w)$ is related to Meixner polynomials.*

Theorem 1. *Polynomials $P_n(w)$ and $Q_n(w)$ satisfy the RH-property (see [3]), namely, all their zeros lie in the line $\mathrm{Re}(z) = 0$.*

Proof. This follows directly from the Jacobi theorem, which states that the tridiagonal matrices of form (3) and (6) are similar to skew-symmetric matrices (for details, see [3]). □

3. Convergence questions

So far we did not consider the convergence of (1). Here we can apply the following theorem:

Theorem 2 (Van Vleck). *Let $\epsilon > 0$. Continued fraction $\mathbf{K}_{r=1}^{\infty}(\frac{1}{b_r})$ (see (1) for the notation), where $-\frac{\pi}{2} + \epsilon < \arg(b_r) < \frac{\pi}{2} - \epsilon$ converges (to a finite value) if and only if the series*

$$\sum_{r=1}^{\infty} |b_r| \tag{5}$$

diverges.

We can apply the theorem by rewriting (1) in an equivalent form

$$\mathfrak{D}(w) = -w + \cfrac{1}{-w/1 + \cfrac{1}{-w/4 + \cfrac{1}{-4w/9 + \cfrac{1}{-9w/64 + \cfrac{1}{-64w/225 + \ddots}}}}}, \tag{6}$$

which, using the notation in (1) can be written as $-w + \mathbf{K}_{r=1}^{\infty}(\frac{1}{-\xi_r w})$, where $\xi_r = (\frac{(r-1)!!}{r!!})^2$.

If $r = 2k$ is even, we can estimate

$$\frac{(r-1)!!}{r!!} = \frac{2k!}{2^k k!} : 2^k k! = \frac{1}{2^{2k}}\binom{2k}{k} \sim \frac{1}{\sqrt{\pi k}},$$

and the estimate is similar for odd r. Therefore, $\xi_r = \Theta(\frac{1}{r})$ and the series (5) with $b_r = \xi_r w$ obviously diverges whenever $w \neq 0$. It follows that the continued fraction expansion (1) is convergent for all $w \neq 0$, provided $\arg b_r \neq \pm\frac{\pi}{2}$.

References

[1] V.P. Il'in, Yu. I. Kuznetsov, Tridiagonal matrices and their applications. Nauka, Moscow, 1985.

[2] Wikipedia: Tridiagonal matrix. https://en.wikipedia.org/wiki/Tridiagonal_matrix. Downloaded March 29 2021.

[3] N. Gogin and M. Hirvensalo, *Riemann Hypothesis Analog for the Krawtchouk and Discrete Chebyshev Polynomials.* Journal of Mathematical Sciences, Vol. 507, pp. 709–716, 2021.

[4] Wikipedia: *Generalized continued fraction.* `https://en.wikipedia.org/wiki/Generalized_continued_fraction`

[5] Jones, William B., Thron, W. J.: *Continued Fractions: Analytic Theory and Applications.* Encyclopedia of Mathematics and its Applications vol. 11, Reading. Massachusetts: Addison-Wesley Publishing Company, (1980), ISBN 0-201-13510-8

[6] P. Flajolet: *Combinatorial Aspects of Continued Fractions.* Discrete Mathematics 32 (1980) 125-161. North-Holland Publishing Company

Nikita Gogin

Mika Hirvensalo
Department of Mathematics and Statistics
University of Turku
Turku, Finland
e-mail: `mikhirve@utu.fi`

Teaching Math in SGU with Computer Algebra Systems

Stefan Hypolite James and Tatiana Mylläri

Abstract. We discuss usage of computer algebra systems in teaching College Mathematics in St. George's University. Some examples are given.

Introduction

St. George's University School of Arts and Sciences comprise mainly of local and Caribbean students. From our lens in Grenada, students display a negative perception of Mathematics at all levels in their academic journey, from primary, secondary and tertiary level education. Many variables are responsible for the learning of mathematics. These factors include but are not limited to: teachers, students, environment and classroom setting; teachers must lead this process.

We agree with the ideas presented in [1, 2]: modern computer algebra systems (CAS) change the way to do mathematics and to teach mathematics. Some of our experience of using CAS in education was described earlier [5, 6]. We believe that with the introduction of technology in mathematics classroom students' performance will improve. We selected the use of two Computer Algebra Systems: Maxima and GeoGebra for teaching Mathematics at St. George's University; both programs are free with an excellent user graphic interface for its users.

Grenada as a third world country has limited resources with low income as compared to the other developing countries. The cost to students will be zero, Students, will not incur any cost to use CAS in the learning environment in SGU.

To assist students, we have created a Power Point presentation with instructions for the use of both Maxima and GeoGebra. Students will also have the advantage of checking for accuracy as well as to generate additional examples in order to achieve mastery in various Math topics. Polya's Problem Solving Technique can be incorporated by SGU students in the learning environment for mathematics:

1. Identify the problem (Identify and understand the problem)
2. Devise a plan (Use Maxima/ GeoGebra)

3. Carryout the Plan (Correctly input the information in Maxima / GeoGebra; use the power point for assistance) CAS
4. Check-Back (Check physical workings with CAS answers).

Teachers are stagnated with the method in which math is taught in the Caribbean. We believe that with the use of technology students will be motivated to learn Math concepts in the learning environment. Teachers can also use CAS to generated additional examples for students as well as it can positively assist with the explanations of complicated Math problems; teachers do not have to waste time on problems that are difficult from the computational point of view. Topics which can be incorporated with the use of CAS: basic simplification, factorization, solving polynomial equations, solving linear systems with 2, 3 and more variables, matrices (determinant of 3x3 and inverse of a matrix), Geometry (area, perimeter and volume of shapes), and others. Below, we give just a few examples of how we are using CAS in the classroom.

1. Examples with Maxima

Certainly, Mathematica or Maple would be even better to use in the classroom, but Maxima can do most of things needed and as it was mentioned earlier, Maxima is free. Some examples and discussion of using Maxima in education can be found in [3, 4].

Maxima easily allows calculation of the determinant of Matrix A or finding the inverse of the matrix (Figure 1). It is very easy to solve quadratic equation

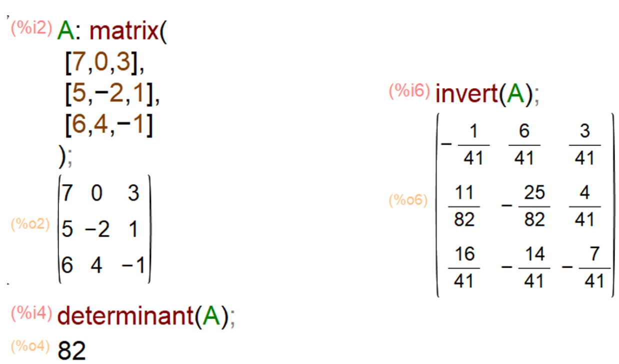


Figure 1. Calculation of the determinant and inverse of matrix A

and illustrate solutions with a plot (Figure 2). It is also easy to solve systems of linear equations and in the case of two equations with two variables to illustrate it (Figure 3).

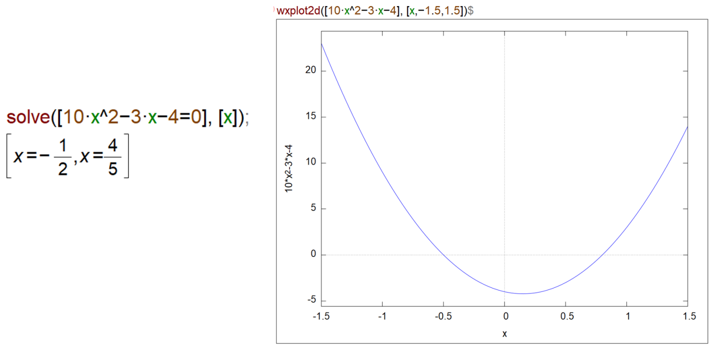


FIGURE 2. Solution of Quadratic Equation

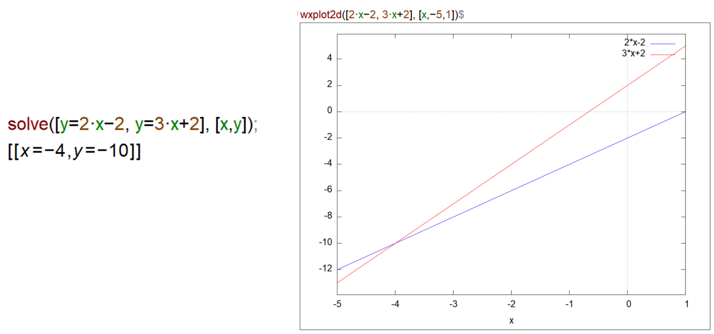


FIGURE 3. Solution of Linear System

2. Some examples with GeoGebra

GeoGebra is useful not only for solving problems, but also for preparing illustrations, demonstrations and experimenting. Some basic examples are shown on figures 5, 4, and 6.

Conclusion

Using CAS helps students to deal with complicated problems, lets students to check results obtained by hand. Teacher can use CAS for demonstrations during the lecture and for preparing students' assignments. We believe that using CAS in the classroom will improve the quality of teaching mathematics.

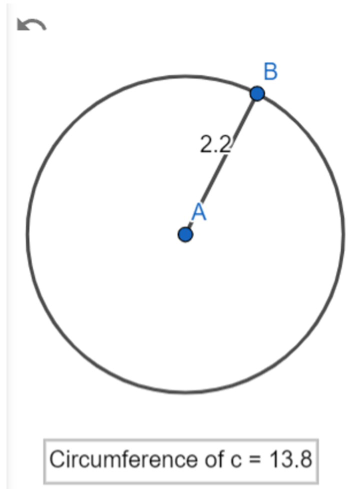


FIGURE 4. Circumference of a circle

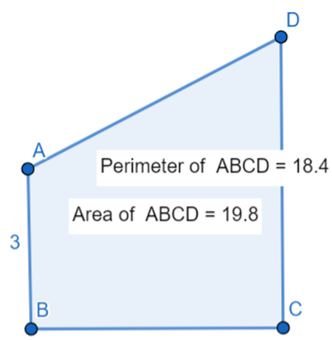


FIGURE 5. Finding of area and perimeter of a trapezium

References

[1] Vavilov N. A. *Computers as fresh mathematical reality. I. Personal account. Computer Tools in Education (2)*, pp. 5-26, 2020.

[2] Vavilov N. A., Halin V.G., Yurkov A. V. *Mathematica for non-mathematician:* University textbook, Moscow, 2021 (in Russian)

[3] Karjanto, N., Husain, H. S. *Adopting Maxima as an Open-Source Computer Algebra System into Mathematics Teaching and Learning,* Proceedings of the 13th International Congress on Mathematical Education, pp. 733-734, Springer International Publishing, 2017.

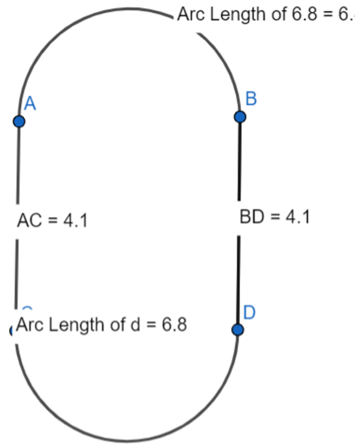


FIGURE 6. Calculation of perimeter

[4] Fedriani, E. M., Moyano, R. *Using Maxima in the Mathematics Classroom.* International Journal for Technology in Mathematics Education, Vol. 18 Issue 4, pp. 171-176, 2011.

[5] Mylläri A., Mylläri T., Cummings T. *Using CAS in teaching basic Calculus.* In Abstracts for the International Conference Mathematical Partnership, Parallel Computing and Computer Algebra, MathParCA - 2014, Mochlos, Crete, Greece, pp. 36 - 39, 2014.

[6] Hypolite S., Mylläri A. *Use Of Computer Algebra Systems In Teaching Math At SGU.* Computer tools in education, pp. 96 - 100, No 3, 2021.

Stefan Hypolite James
SAS
St.George's University
St.George's, Grenada, West Indies
e-mail: `shypolit@sgu.edu`

Tatiana Mylläri
SAS
St.George's University
St.George's, Grenada, West Indies
e-mail: `tmyllari@sgu.edu`

Is there an algebraic geometry for exponential sums?

B. Kazarnovskii

Abstract. An analytic set in $\mathbb{C}^n$, given as the zero set of a finite system of exponential sums, is said to be the exponential variety (E-variety). We define the intersection number for any two E-varieties. The main problem in this definition is the infinity of a 0-dimensional E-variety (as for the zero set of $e^z - 1$). To overcome this obstacle, we introduce the concept of weak density, which is analogous to the number of points of a 0-dimensional algebraic variety.

Introduction

An exponential sum (ES) is a function on $\mathbb{C}^n$ of the form

$$f(z) = \sum_{\lambda\in\Lambda,\ c_\lambda\in\mathbb{C}} c_\lambda\, e^{\langle z,\lambda\rangle},$$

where Λ is a finite set in $\mathbb{C}^n$, and $\langle z,\lambda\rangle = z_1\overline{\lambda}_1 + \ldots + z_n\overline{\lambda}_n$. The sets Λ and $\operatorname{conv}(\Lambda)$ are respectively called the *support* and the *Newton polytope* of ES. Below we assume that $\lambda_i \in \mathbb{R}$. Thus Newton polytope is a convex polytope in $\mathbb{R}^n$.

The ring of ESs looks like a Laurent polynomial ring. In 1929 J. Ritt proved that, if the ratio of two ESs in one variable is an entire function, then this function is also an ES. (Ritt multidimensional theorem was proved later.) However, many attempts to find other algebraic-geometric properties, similar to the properties of the ring of polynomials, encountered great difficulties. For example, the existence of a common zero of two ESs does not imply the existence of a common divisor: the ESs $e^z - 1,\ e^{\sqrt{2}z} - 1$, having a common zero at $z = 0$ have no a common divisor. This follows from the infinity of the zero set of any ES. It is probable that Ritt himself proposed the conjecture about the finiteness of the set of common zeros of two coprime ESs in one variable. Currently, this conjecture is very far from being proven. If one of the ESs is $e^z - 1$, then the conjecture is true. This is the classical result of Skolem on Diophantine solutions of exponential equations. This follows from a theorem called the "Mordell-Lang conjecture" for a complex torus.

Description of results

There has been some progress in the algebra of ESs in recent years; see [3, 4, 5, 6]. The main result is the construction of the "ring of conditions" for the space $\mathbb{C}^n$. The ring of conditions is the ring of the intersection theory on spherical varieties; see [2, 1]. It turned out that a similar intersection theory can be constructed for E-varieties in $\mathbb{C}^n$.

The construction of the ring of conditions is based on the concept of intersection indices of E-varieties. In the talk, we define the weak density of 0-dimensional E-variety, which is analogous to the number of points of a 0-dimensional algebraic variety, and then use the weak density to define the intersection numbers. It turns out that, as in polynomial case, the intersection index of n exponential hypersurfaces is equal to the mixed volume of their Newton polytopes.

Given the intersection indices, it is easy to define the ring of conditions. By definition, the elements of the ring of conditions are the numerical equivalence classes of E-varietes with the "union" and "intersect" operations. However, proving the correctness of the definition is technically quite difficult. We will not consider the details and justify the correctness of this definition during the talk.

References

[1] C. De Concini. *Equivariant embeddings of homogeneous spaces*, Proceedings of the International Congress of Mathematicians, Berkeley, California, USA (1986), 369–377.

[2] C. De Concini and C. Procesi. *Complete symmetric varieties II*, Intersection theory. Adv. Stud. Pure Math., 6 (1985), 481–512.

[3] B. Ya. Kazarnovskii. *Exponential analytic sets*, Funct. Anal. Appl., (31:2), 1997, 86–94

[4] B. Zilber. *Exponential sums equations and the Shanuel conjecture*. Journal of the London Math. Society, (65:2), 2002, 27–44

[5] B. Ya. Kazarnovskii, A.G. Khovanskii, and A. I. Esterov. *Newton polytopes and tropical geometry*, Russian Mathematical Surveys, 2021, 76:1, 91–175

[6] Kazarnovskii, B. Ya. *The quasi-algebraic ring of conditions of* $\mathbb{C}^n$, Izvestiya: Mathematics (2022), (86:1), 169–202

B. Kazarnovskii
Institute for Information Transmission Problems
Moscow
e-mail: kazbori@gmail.com

Symplectic Structures in Finite Quantum Mechanics and Generalized Clifford Algebras

Vladimir V. Kornyak

Abstract. In the Hamiltonian formulation of classical mechanics, the state of a system is described by pairs of conjugate variables q and p called *positions* and *momenta*. These pairs form an even-dimensional *symplectic* manifold.

When constructing quantum mechanics, the variables q and p are naturally replaced with Hermitian operators $\hat{q}$ and $\hat{p}$ that must satisfy the Heisenberg *canonical commutation relation* $[\hat{q}, \hat{p}] = \mathbf{i}\hbar$, without which it is impossible to describe quantum interference. However, this relation is not fundamental. Being, in fact, an infinitesimal approximation of a more fundamental relation, it can only be realized in an infinite-dimensional Hilbert space. Replacing the conjugate *Hermitian* operators $\hat{q}$ and $\hat{p}$ with a pair of *unitary* operators Q and P, Hermann Weyl constructed a canonical commutation relation

$$QP = \omega PQ,\ \omega = \mathrm{e}^{2\pi\mathbf{i}/N}\,.$$

Weyl proved that the matrices Q and P are generators of a projective representation of $\mathbb{Z}_N \times \mathbb{Z}_N$ in the N-dimensional Hilbert space and coincide with "the shift and clock matrices" discovered by J.J. Sylvester in the 19th century. The shift matrix Q is the matrix of cyclic permutation of N elements. The clock matrix P is simply the diagonal form of the matrix Q.

The orthonormal bases associated with the matrices Q and P are *mutually unbiased bases*, a concept that is a deep quantum version of the symplectic conjugation introduced by J. Schwinger.

The matrices Q and P generate a structure called the *generalized Clifford algebra*. This structure is quite non-trivial and even in the simplest case $N = 2$ allows one to describe quaternions, three-dimensional rotations, spin-$\frac{1}{2}$ particles, etc. Thus, having only single cyclic permutation of N elements, using purely mathematical means — linear algebra, projective representations and central group extensions — we get rich tools for studying quantum-mechanical problems.

The fundamental role of the cyclic permutation matrix Q agrees well with the *finite quantum mechanics* [1–3] describing unitary evolutions by permutations, which are always products of cyclic permutations.

References

[1] Kornyak V.V. *Quantum models based on finite groups.* IOP Conf. Series: Journal of Physics: Conf. Series **965**, 012023, 2018. arXiv:1803.00408 [physics.gen-ph]

[2] Kornyak V.V. *Modeling Quantum Behavior in the Framework of Permutation Groups.* EPJ Web of Conferences **173**, 01007, 2018. arXiv:1709.01831 [quant-ph]

[3] Kornyak V.V. *Mathematical Modeling of Finite Quantum Systems.* In: Adam G. *et al* (eds) MMCP 2011. LNCS, **7125**. Springer, 2012. arXiv:1107.5675 [quant-ph]

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

Tropical Optimization Techniques for Solving Multicriteria Problems in Decision Making

Nikolai Krivulin

Abstract. We consider a decision-making problem to find ratings of alternatives from pairwise comparisons under several criteria, subject to constraints imposed on the ratings. Given matrices of pairwise comparisons, the problem is formulated as the log-Chebyshev approximation of these matrices by a common consistent matrix (a symmetrically reciprocal matrix of unit rank) that minimizes the approximation errors for all matrices simultaneously. We rearrange the approximation problem as a constrained multiobjective optimization problem of finding a vector that determines the approximating matrix. The optimization problem is then represented in the framework of tropical algebra. We apply methods and results of tropical optimization to solve the problem according to various principles of optimality, including the max-ordering, lexicographic ordering and lexicographic max-ordering optimality.

Introduction

Tropical optimization constitutes an important research and application domain of tropical (idempotent) mathematics [1, 2, 3], which focuses on optimization problems that are formulated and solved in the framework of semirings and semifields with idempotent addition. Methods and techniques of tropical optimization find application in many areas, including engineering, computer science and operations research, where they offer new solutions to various classical and novel problems. As an application example one can consider decision-making problems of deriving priorities of alternatives from pairwise comparisons [4, 5, 6].

In this paper, we consider a decision-making problem to find absolute ratings (scores, priorities, weights) of alternatives, which are compared in pairs under several criteria, subject to constraints in the form of two-sided bounds (box-constraints) on ratios between the ratings. Given matrices of pairwise comparisons made according to the criteria, the problem is formulated as the log-Chebyshev approximation of these matrices by a common consistent matrix (a symmetrically reciprocal matrix of unit rank) that minimizes the approximation errors for all matrices simultaneously. We rearrange the approximation problem as a constrained multiobjective optimization problem of finding a vector that determines the approximating consistent matrix.

The optimization problem is then represented in the framework of tropical algebra. We apply methods and results of tropical optimization to handle the multiobjective optimization problem according to various principles of optimality [7, 8]. Complete solutions in the sense of the max-ordering, lexicographic ordering and lexicographic max-ordering optimality are obtained, which are given in a compact vector form ready for formal analysis and efficient computation.

1. Single-Criterion Pairwise Comparison Problem

Suppose that n alternatives are compared in pairs, which results in a pairwise comparison matrix $\boldsymbol{C} = (c_{ij})$ where the entry $c_{ij} > 0$ shows that alternative i is c_{ij} times more preferable than alternative j. The matrix $\boldsymbol{C}$ is assumed to be symmetrically reciprocal, which means that $c_{ij} = 1/c_{ji}$ for all $i, j = 1, \ldots, n$. Given a pairwise comparison matrix $\boldsymbol{C}$, the problem of interest is to calculate individual ratings (scores, priorities, weights) of alternatives.

A pairwise comparison matrix $\boldsymbol{C}$ is referred to as consistent if the condition $c_{ij} = c_{ik}c_{kj}$ holds for all i, j, k. If a pairwise comparison matrix $\boldsymbol{C}$ is consistent, then it is not difficult to verify that there exists a positive vector $\boldsymbol{x} = (x_i)$ whose entries determine the entries of $\boldsymbol{C}$ by the relation $c_{ij} = x_i/x_j$ valid for all i, j. It directly follows from this relation that the vector $\boldsymbol{x}$, which is defined up to a positive factor, can be taken as a vector of absolute ratings of alternatives and thus gives the solution of the pairwise comparison problem.

The matrices of pairwise comparisons that appear in real-world problems are commonly not consistent, which makes the problem of evaluating absolute ratings nontrivial. The solution techniques available to handle the problem include heuristic methods that do not guarantee the optimality of solution, but offer results acceptable in practice, and approximation methods that provide mathematically justified optimal solutions, which however can involve difficult computations.

An approximation technique that minimizes the Chebyshev distance in logarithmic scale (a log-Chebyshev approximation) are proposed in [4]. The method is to find positive vectors $\boldsymbol{x} = (x_i)$ that solve the problem

$$\min_{\boldsymbol{x}>\boldsymbol{0}} \quad \max_{1\leq i,j\leq n} \left| \log c_{ij} - \log \frac{x_i}{x_j} \right|.$$

Suppose now that there are constraints imposed on the absolute ratings of alternatives in the form of two-sided bounds on ratios between the ratings. Given a matrix $\boldsymbol{B} = (b_{ij})$ where $b_{ij} \geq 0$ shows that alternative i must be considered not less than b_{ij} times better than j, the constraints are given by the inequalities

$$\max_{1\le j\le n} b_{ij}x_j \le x_i, \qquad i=1,\dots,n.$$

Observing that the logarithm to a base greater than 1 monotonically increases, one can rewrite the objective function in the problem as

$$\max_{1\le i,j\le n}\left|\log c_{ij} - \log\frac{x_i}{x_j}\right| = \log \max_{1\le i,j\le n}\frac{c_{ij}x_j}{x_i}.$$

The logarithmic function on the left-hand side attains its maximum where its argument is maximal, which allows us to remove the logarithm from the objective function to solve the equivalent problem

$$\begin{aligned} \min_{\boldsymbol{x}>\boldsymbol{0}} \quad & \max_{1\le i,j\le n}\frac{c_{ij}x_j}{x_i}; \\ \text{s.t.} \quad & \max_{1\le j\le n} b_{ij}x_j \le x_i, \qquad i=1,\dots,n. \end{aligned}$$

2. Multicriteria Pairwise Comparison Problems

Assume that n alternatives are compared in pairs according to m criteria. For each criterion $l=1,\dots,m$, the results of pairwise comparisons are given by a matrix $\boldsymbol{C}_l=(c_{ij}^{(l)})$ of order n. The problem is to find a vector $\boldsymbol{x}=(x_i)$ of ratings subject to constraints given by a matrix $\boldsymbol{B}=(b_{ij})$ of order n. Application of the log-Chebyshev approximation technique yields the problem

$$\begin{aligned} \min_{\boldsymbol{x}>\boldsymbol{0}} \quad & \left(\max_{1\le i,j\le n}\frac{c_{ij}^{(1)}x_j}{x_i},\dots,\max_{1\le i,j\le n}\frac{c_{ij}^{(m)}x_j}{x_i}\right); \\ \text{s.t.} \quad & \max_{1\le j\le n} b_{ij}x_j \le x_i, \qquad i=1,\dots,n. \end{aligned} \tag{1}$$

In the rest of this section, we consider three common approaches to handle problem (1), which result in different procedures to find the solution set X. The solution techniques used are based on the max-ordering, lexicographic ordering and lexicographic max-ordering principles of optimality [7].

2.1. Max-Ordering Solution

Max-ordering optimization aims at minimizing the worst value of the objective functions, and leads to replacing the vector of objective functions by a scalar function given by the maximum of the objective functions (Chebyshev scalarization).

To solve the constrained problem at (1), we define the feasible solution set

$$X_0=\left\{\boldsymbol{x}>\boldsymbol{0}\ :\ \max_{1\le j\le n} b_{ij}x_j\le x_i, \quad i=1,\dots,n\right\}.$$

We apply the Chebyshev scalarization to form the objective function

$$\max_{1\le l\le m}\max_{1\le i,j\le n}\frac{c_{ij}^{(l)}x_j}{x_i} = \max_{1\le i,j\le n}\frac{c_{ij}x_j}{x_i}, \qquad c_{ij}=\max_{1\le l\le m} c_{ij}^{(l)}.$$

Then, the problem reduces to the constrained minimization problem

$$\min_{\boldsymbol{x}\in X_0} \quad \max_{1\leq i,j\leq n} \frac{c_{ij}x_j}{x_i},$$

which is to solve to obtain the max-ordering solution as the set

$$X_1 = \arg\min_{\boldsymbol{x}\in \boldsymbol{X}_0} \max_{1\leq i,j\leq n} \frac{c_{ij}x_j}{x_i}.$$

Note that the solution obtained by the max-ordering optimization is known to be week Pareto-optimal, and becomes Pareto optimal if it is unique [8].

2.2. Lexicographic Ordering Solution

Lexicographic optimization considers the objective functions in a hierarchical order based on some ranking of objectives. Suppose the objectives are numbered in such a way that objective 1 has the highest rank, objective 2 has the second highest and so on. The lexicographic approach first minimizes function 1 and examine the set of solutions obtained. If the solution obtained is unique (up to a positive factor), it is taken as the solution of the overall multiobjective problem. Otherwise function 2 is minimized over all solutions of the first problem, and the procedure continues until a unique solution is obtained or the problem with function m is solved.

To apply this approach, we first take the initial feasible solution set X_0 defined above, and then obtain the solution set X_s for each problem

$$\min_{\boldsymbol{x}\in X_{s-1}} \quad \max_{1\leq i,j\leq n} \frac{c_{ij}^{(s)}x_j}{x_i}, \qquad s = 1,\ldots,m.$$

The solution procedure stops as soon as the set X_s consists of a single solution vector or all m scalar objective functions are examined. The last found set X_s is taken as the lexicographic solution for the problem.

2.3. Lexicographic Max-Ordering Solution

This approach combines the lexicographic ordering and max-ordering into one procedure that improves the accuracy of the assessment provided by the max-ordering approach. The procedure consists of several steps, each of which finds the max-ordering solution of a reduced problem that has a lower multiplicity of objectives and smaller feasible set. The first solution step coincides with the above described max-ordering solution of the constrained problem with m objectives and the feasible solution set given by the constraints. Each subsequent step takes the solution from the previous step as a current feasible solution set and selects objectives that can be further minimized over the current feasible set, to incorporate into the current vector objective function. A scalar objective function is included in the current function if it has its minimum value over the current feasible set below the minimum of the objective function at the previous step.

To describe the solution, we use the symbol I_s to denote the set of indices of scalar objective functions involved at step s. We initially set $I_0 = \{1,\ldots,m\}$ and define X_0 as above. At each step s, we need to solve the problem

$$\min_{\boldsymbol{x}\in X_{s-1}} \quad \max_{l\in I_{s-1}} \max_{1\leq i,j\leq n} \frac{c_{ij}^{(l)} x_j}{x_i}, \qquad s = 1,\dots,m.$$

where X_{s-1} denotes the solution set of the problem at step $s-1$.

With the minimum value of the objective function at step s denoted by θ_s, we define the index set as follows:

$$I_s = \left\{ l \in I_{s-1} :\ \theta_s > \min_{\boldsymbol{x}\in X_s} \max_{1\leq i,j\leq n} \frac{c_{ij}^{(l)} x_j}{x_i} \right\}.$$

The procedure is completed if either the set X_s reduces to a single solution vector, the condition $I_s = \emptyset$ holds or all m objective functions are examined.

Below, we show how the solutions offered by the above methods can be represented in explicit analytical form using methods and result of tropical mathematics.

3. Preliminary Algebraic Definitions and Notation

Consider a tropical (idempotent) semifield that is defined as the set of nonnegative reals equipped with addition $\oplus$ given by the maximum as $x \oplus y = \max(x, y)$, and multiplication denoted and defined as usual. Addition is idempotent since $x \oplus x = \max(x, x) = x$, and has 0 as the neutral element. Multiplication has 1 as the neutral element, is invertible for all nonzero x and distributes over addition. This tropical semifield is commonly referenced to as the max-algebra.

Matrices and vectors over the max-algebra are routinely introduced. Matrix and vector operations follow the standard entrywise rules with the scalar addition $+$ replaced by $\oplus$. The conjugate of a column vector $\boldsymbol{x} = (x_j)$ is the row vector $\boldsymbol{x}^- = (x_j^-)$ where $x_j^- = x_j^{-1}$ if $x_j \neq 0$, and $x_j^- = 0$ otherwise. The zero vector is denoted by $\mathbf{0}$, and identity matrix by $\boldsymbol{I}$. For any square matrix, the power notation indicates repeated (tropical) multiplication of the matrix by itself.

For any square matrix $\boldsymbol{A} = (a_{ij})$ of order n, the trace is given by

$$\operatorname{tr} \boldsymbol{A} = a_{11} \oplus \cdots \oplus a_{nn}.$$

A tropical analogue of the matrix determinant is defined as

$$\operatorname{Tr}(\boldsymbol{A}) = \operatorname{tr} \boldsymbol{A} \oplus \cdots \oplus \operatorname{tr} \boldsymbol{A}^n.$$

If $\operatorname{Tr}(\boldsymbol{A}) \leq 1$, then the Kleene star operator is calculated as

$$\boldsymbol{A}^* = \boldsymbol{I} \oplus \boldsymbol{A} \oplus \cdots \oplus \boldsymbol{A}^{n-1}.$$

4. Solution of Multicriteria Pairwise Comparison Problems

Consider the multiobjective optimization problem at (1). After rewriting the objective functions and inequality constraints in terms of max-algebra, the problem can be formulated in vector form as follows. Given $(n \times n)$-matrices $\boldsymbol{C}_l$ of pairwise comparisons of n alternatives for criteria $l = 1, \ldots, m$, and nonnegative $(n \times n)$-matrix $\boldsymbol{B}$ of constraints, find positive n-vectors $\boldsymbol{x}$ of ratings that solve the problem

$$\begin{aligned} \min_{\boldsymbol{x} > \boldsymbol{0}} \quad & (\boldsymbol{x}^{-} \boldsymbol{C}_1 \boldsymbol{x}, \ldots, \boldsymbol{x}^{-} \boldsymbol{C}_m \boldsymbol{x}); \\ \text{s.t.} \quad & \boldsymbol{B} \boldsymbol{x} \leq \boldsymbol{x}. \end{aligned} \tag{2}$$

Below, we offer max-ordering, lexicographic and lexicographic max-ordering optimal solutions to this problem.

4.1. Max-Ordering Solution

We start with a solution obtained according to the max-ordering optimality.

Theorem 1. *Let $\boldsymbol{C}_l$ for all $l = 1, \ldots, m$ be matrices such that* $\mathrm{Tr}(\boldsymbol{C}_l) \neq 0$*, and $\boldsymbol{B}$ be a matrix such that* $\mathrm{Tr}(\boldsymbol{B}) \leq 1$. *With $\boldsymbol{A} = \boldsymbol{C}_1 \oplus \cdots \oplus \boldsymbol{C}_m$, define the scalar*

$$\theta = \bigoplus_{k=1}^{n} \bigoplus_{0 \leq i_1 + \cdots + i_k \leq n-k} \mathrm{tr}^{1/k} (\boldsymbol{A} \boldsymbol{B}^{i_1} \cdots \boldsymbol{A} \boldsymbol{B}^{i_k})$$

and matrix

$$\boldsymbol{G} = (\theta^{-1} \boldsymbol{A} \oplus \boldsymbol{B})^{*}.$$

Then, all max-ordering solutions of problem (2) *are given in parametric form by*

$$\boldsymbol{x} = \boldsymbol{G} \boldsymbol{u}, \qquad \boldsymbol{u} \neq \boldsymbol{0}.$$

4.2. Lexicographic Ordering Solution

The lexicographic ordering technique solves problem (2) in m steps each minimizing a scalar objective function over a feasible set given by the previous step.

Theorem 2. *Let $\boldsymbol{C}_l$ for all $l = 1, \ldots, m$ be matrices such that* $\mathrm{Tr}(\boldsymbol{C}_l) \neq 0$*, and $\boldsymbol{B}$ be a matrix such that* $\mathrm{Tr}(\boldsymbol{B}) \leq 1$. *With $\boldsymbol{B}_0 = \boldsymbol{B}$, define the recurrence relations*

$$\begin{aligned} \theta_s &= \bigoplus_{k=1}^{n} \bigoplus_{0 \leq i_1 + \cdots + i_k \leq n-k} \mathrm{tr}^{1/k} (\boldsymbol{C}_s \boldsymbol{B}_{s-1}^{i_1} \cdots \boldsymbol{C}_s \boldsymbol{B}_{s-1}^{i_k}), \\ \boldsymbol{B}_s &= \theta_s^{-1} \boldsymbol{C}_s \oplus \boldsymbol{B}_{s-1}, \qquad s = 1, \ldots, m; \end{aligned}$$

and the matrix

$$\boldsymbol{G} = \boldsymbol{B}_m^{*}.$$

Then, all max-ordering solutions of problem (2) *are given by*

$$\boldsymbol{x} = \boldsymbol{G} \boldsymbol{u}, \qquad \boldsymbol{u} \neq \boldsymbol{0}.$$

4.3. Lexicographic Max-Ordering Solution

Similar to the lexicographic ordering solution, we handle problem (2) by solving a series of problems, where each problem has a scalar objective function and inequality constraint provided by the solution of the previous problems. The solution obtained in the framework of max-algebra is described as follows.

Theorem 3. *Let* $\boldsymbol{C}_l$ *for all* $l = 1, \ldots, m$ *be matrices such that* $\mathrm{Tr}(\boldsymbol{C}_l) \neq 0$*, and* $\boldsymbol{B}$ *be a matrix such that* $\mathrm{Tr}(\boldsymbol{B}) \leq 1$*. With* $\boldsymbol{B}_0 = \boldsymbol{B}$ *and* $I_0 = \{1, \ldots, m\}$*, define the recurrence relations*

$$\theta_s = \bigoplus_{k=1}^{n} \bigoplus_{0 \leq i_1 + \cdots + i_k \leq n-k} \mathrm{tr}^{1/k}(\boldsymbol{A}_s \boldsymbol{B}_{s-1}^{i_1} \cdots \boldsymbol{A}_s \boldsymbol{B}_{s-1}^{i_k}), \qquad \boldsymbol{A}_s = \bigoplus_{l \in I_{s-1}} \boldsymbol{C}_l,$$

$$I_s = \left\{ l \in I_{s-1} \ : \ \theta_s > \bigoplus_{k=1}^{n} \bigoplus_{0 \leq i_1 + \cdots + i_k \leq n-k} \mathrm{tr}^{1/n}(\boldsymbol{C}_l \boldsymbol{B}_s^{i_1} \cdots \boldsymbol{C}_l \boldsymbol{B}_s^{i_k}) \right\},$$

$$\boldsymbol{B}_s = \theta_s^{-1} \boldsymbol{A}_s \oplus \boldsymbol{B}_{s-1}, \qquad s = 1, \ldots, m;$$

and the matrix

$$\boldsymbol{G} = \boldsymbol{B}_m^{*}.$$

Then, all lexicographic max-ordering solutions of problem (2) *are given by*

$$\boldsymbol{x} = \boldsymbol{G}\boldsymbol{u}, \qquad \boldsymbol{u} \neq \boldsymbol{0}.$$

References

[1] V. N. Kolokoltsov, V. P. Maslov. *Idempotent Analysis and Its Applications*, Mathematics and Its Applications, Vol. 401. Dordrecht, Springer, 1997.

[2] J. S. Golan. *Semirings and Affine Equations Over Them*, Mathematics and Its Applications, Vol. 556. Dordrecht, Springer, 2003.

[3] B. Heidergott, G. J. Olsder, J. van der Woude. *Max Plus at Work*, Princeton Series in Applied Mathematics. Princeton, NJ, Princeton Univ. Press, 2006.

[4] N. Krivulin, S. Sergeev. Tropical implementation of the Analytical Hierarchy Process decision method // *Fuzzy Sets and Systems.* 2019. Vol. 377. P. 31–51.

[5] N. Krivulin. Using tropical optimization techniques in bi-criteria decision problems // *Comput. Manag. Sci.* 2020. Vol. 17, N 1. P. 79–104.

[6] N. Krivulin. Algebraic solution to constrained bi-criteria decision problem of rating alternatives through pairwise comparisons // *Mathematics.* 2021. Vol. 9, N 4. P. 303.

[7] M. Ehrgott. *Multicriteria Optimization*, 2 ed. Berlin, Springer, 2005.

[8] H. Nakayama, Y. Yun, M. Yoon. *Sequential Approximate Multiobjective Optimization Using Computational Intelligence*, Springer Series in Vector Optimization. Berlin, Springer, 2009.

Nikolai Krivulin
Faculty of Mathematics and Mechanics
St. Petersburg State University
St. Petersburg, Russia
e-mail: `nkk@math.spbu.ru`

Solving the problem of choosing an information system project by methods of tropical mathematics

Nikolai Krivulin and Alexey Prinkov

Abstract. A multicriteria problem of evaluating the ratings of alternatives based on pairwise comparisons when making a decision on choosing an information system project is considered. To solve the problem, an approach based on the weighted minimax log-Chebyshev approximation and the application of tropical mathematics methods are used. The obtained solution is compared with the known solution by the method of analytical hierarchy process.

Introduction

Multicriteria problems of evaluating alternatives based on pairwise comparisons are significant class of decision-making problems that are common in many areas. In multicriteria problems, the alternatives are compared in accordance with several criteria. The main difficulty of such problems is the absence in the general case of a solution that is the best for all criteria at once. The initial data for the problem are a set of m alternatives and their pairwise comparison by n criteria. The results of comparisons are represented in the form of pairwise comparisons matrices $\boldsymbol{A}_k$, where $1 \leq k \leq n$. The criteria are also compared with each other in pairs, and the results of the comparisons are recorded in a criteria comparisons matrix $\boldsymbol{C}$. The solution of the problem is the vector of absolute ratings, which determines the ranks of alternatives. One of the approaches to solve the problem is based on the log–Chebyshev approximation of pairwise comparisons matrices by consistent matrices (inversely symmetric matrices of unit rank). The log-Chebyshev approximation problem can be represented in terms of tropical mathematics and then solved analytically in a compact vector form.

1. Algebraic definitions

Tropical (idempotent) mathematics studies the theory and applications of algebraic systems with idempotent operations [1, 2, 3]. An operation is called idempotent if, when applied to the same arguments, it results in this argument. For example, the maximum operation is idempotent: $\max(x, x) = x$. Optimization problems formulated in terms of idempotent algebraic systems can be solved by methods of tropical optimization.

The paper uses max–algebra, an algebraic system, which is a set of non-negative real numbers $\mathbb{R}_+ = \{x \in \mathbb{R} | x \leq 0\}$ with addition and multiplication operations. Addition is defined as maximum and denoted by $\oplus$. Multiplication is defined and denoted as usual. Vector and matrix operations are performed according to standard rules with the replacement of arithmetic addition by the operation $\oplus$. The unit matrix is denoted by $\boldsymbol{I}$ and has the usual form. The integer non-negative power of a square matrix $\boldsymbol{A}$ denotes the result of the multiplication of the matrix by itself and is defined for all natural p as $\boldsymbol{A}^0 = \boldsymbol{I}$, $\boldsymbol{A}^p = \boldsymbol{A}^{p-1}\boldsymbol{A} = \boldsymbol{A}\boldsymbol{A}^{p-1}$. The trace of a matrix $\boldsymbol{A} = (a_{ij})$ of order n is calculated by the formula $\operatorname{tr} \boldsymbol{A} = a_{11} \oplus \cdots \oplus a_{nn}$.

The spectral radius of the matrix $\boldsymbol{A}$ is calculated by the formula

$$\lambda = \operatorname{tr} \boldsymbol{A} \oplus \cdots \oplus \operatorname{tr}^{1/n}(\boldsymbol{A}^n) = \bigoplus_{i=1}^{n} \operatorname{tr}^{1/i}(\boldsymbol{A}^i).$$

If $\lambda < 1$, then for the matrix $\boldsymbol{A}$ the Kleene operator is defined

$$\boldsymbol{A}^* = \boldsymbol{I} \oplus \boldsymbol{A} \oplus \cdots \oplus \boldsymbol{A}^{n-1} = \bigoplus_{i=0}^{n-1} \boldsymbol{A}^i.$$

More detailed information on the theory, methods and applications of theoretical mathematics can be found, for example, in [1, 2, 3].

2. Problem of choosing an information system project

Let us consider the problem of choosing an information system project described in [4]. The problem is to choose the most preferable information system project for implementation according to a set of criteria. The paper [4] provides a solution using the analytic hierarchy process of T. Saaty [5].

In the considered problem, a rating scale from 1 to 9 is used. In total, $m = 6$ competing alternative information system projects are considered. Alternatives are compared according to $n = 4$ criteria: increasing the accuracy of clerical operations, the efficiency of information processing, the promotion of organizational learning and the implementation costs.

A pairwise comparisons matrix of criteria is given by:

$$\boldsymbol{C} = \begin{pmatrix} 1 & 1/9 & 1/7 & 1/5 \\ 9 & 1 & 2 & 5 \\ 7 & 1/2 & 1 & 3 \\ 5 & 1/5 & 1/3 & 1 \end{pmatrix}.$$

Pairwise comparisons matrices of alternatives for each criterion are:

$$\boldsymbol{A}_1 = \begin{pmatrix} 1 & 1/3 & 1/6 & 1/6 & 1/3 & 1/9 \\ 3 & 1 & 1/3 & 1/3 & 1 & 1/8 \\ 6 & 3 & 1 & 1 & 3 & 1/8 \\ 6 & 3 & 1 & 1 & 3 & 1/8 \\ 3 & 1 & 1/3 & 1/3 & 1 & 1/8 \\ 9 & 8 & 8 & 8 & 8 & 1 \end{pmatrix}; \qquad \boldsymbol{A}_2 = \begin{pmatrix} 1 & 4 & 3 & 1 & 3 & 4 \\ 1/4 & 1 & 7 & 3 & 1/5 & 1 \\ 1/3 & 1/7 & 1 & 1/5 & 1/5 & 1/6 \\ 1 & 1/3 & 5 & 1 & 1 & 1/3 \\ 1/3 & 5 & 5 & 1 & 1 & 3 \\ 1/4 & 1 & 5 & 3 & 1/3 & 1 \end{pmatrix};$$

$$\boldsymbol{A}_3 = \begin{pmatrix} 1 & 1/5 & 2 & 1/3 & 1/2 & 2 \\ 5 & 1 & 7 & 2 & 3 & 7 \\ 1/2 & 1/7 & 1 & 1/5 & 1/2 & 1 \\ 3 & 1/2 & 5 & 1 & 2 & 5 \\ 2 & 1/3 & 2 & 1/2 & 1 & 3 \\ 1/2 & 1/7 & 1 & 1/5 & 1/3 & 1 \end{pmatrix}; \qquad \boldsymbol{A}_4 = \begin{pmatrix} 1 & 5 & 4 & 2 & 3 & 1/3 \\ 1/5 & 1 & 1/2 & 1/4 & 1/3 & 1/8 \\ 1/4 & 2 & 1 & 1/3 & 1/2 & 1/6 \\ 1/2 & 4 & 3 & 1 & 2 & 1/4 \\ 1/3 & 3 & 2 & 1/2 & 1 & 1/5 \\ 3 & 8 & 6 & 4 & 5 & 1 \end{pmatrix}.$$

We now describe the solution of the problem, which is based on the weighted minimax log-Chebyshev approximation and obtained using methods of tropical optimization proposed in [6, 7].

To solve the problem we use analytical computations in terms of max-algebra which is a tropical semifield with addition defined as maximum.

To determine the weights of the criteria, we first calculate the spectral radius of the matrix $\boldsymbol{C}$ given by

$$\lambda = \operatorname{tr} \boldsymbol{C} \oplus \cdots \oplus \operatorname{tr}^{1/4}(\boldsymbol{C}^4) = (25/9)^{1/3} \approx 1.4057.$$

The calculation of the Kleene star matrix, whose columns generate all the optimal vectors of the weights of the criteria, gives the following result:

$$\boldsymbol{D} = (\lambda^{-1}\boldsymbol{C})^* = \begin{pmatrix} 1 & 1/9\lambda & 2\lambda/25 & \lambda/5 \\ 9\lambda & 1 & 2/\lambda & 5/\lambda \\ 27\lambda/5 & 3/5 & 1 & 3/\lambda \\ 5/\lambda & \lambda/5 & 2/5 & 1 \end{pmatrix}.$$

If the columns in the matrix generate a unique (up to a positive multiplier) vector, this vector is taken as the vector of weights. Otherwise some best and worst differentiating vectors of weights are obtained. As the best (worst) vector of weights, a vector is considered for which the ratio between the maximum and minimum elements is maximal (minimal).

We normalize the columns of the matrix $\boldsymbol{D}$ with respect to the maximum element, which makes the maximum element in each column be equal to 1. In this case, the best solutions corresponds to the columns whose minimum elements are the smallest among all columns, and the worst ones to the vectors whose minimum elements are the largest. The normalized matrix $\boldsymbol{D}$ is equal to

$$\begin{pmatrix} 1/9\lambda & 1/9\lambda & 1/9\lambda & 1/9\lambda \\ 1 & 1 & 1 & 1 \\ 3/5 & 3/5 & \lambda/2 & 3/5 \\ \lambda/5 & \lambda/5 & \lambda/5 & \lambda/5 \end{pmatrix}.$$

The best differentiating vector of weights is the vector

$$\boldsymbol{v} = (1/9\lambda,\ 1,\ 3/5,\ \lambda/5)^{\mathrm{T}},$$

and the worst is vector

$$\boldsymbol{w} = (1/9\lambda,\ 1,\ \lambda/2,\ \lambda/5)^{\mathrm{T}}.$$

Let us take the best differentiating vector of weights $\boldsymbol{v}$ and evaluate a weighted sum

$$\boldsymbol{P} = 1/9\lambda \boldsymbol{A}_1 + \boldsymbol{A}_2 + 3/5\boldsymbol{A}_3 + \lambda/5\boldsymbol{A}_4 =$$
$$= \begin{pmatrix} 1 & 4 & 3 & 1 & 3 & 4 \\ 3 & 1 & 7 & 3 & 9/5 & 21/5 \\ 2/3\lambda & 2\lambda/5 & 1 & 1/5 & 3/10 & 3/5 \\ 9/5 & 4\lambda/5 & 5 & 1 & 6/5 & 3 \\ 6/5 & 5 & 5 & 1 & 1 & 3 \\ 3\lambda/5 & 8\lambda/5 & 6 & 3 & \lambda & 1 \end{pmatrix}.$$

The spectral radius of the matrix $\boldsymbol{P}$ is defined as

$$\mu = \operatorname{tr} \boldsymbol{P} \oplus \cdots \oplus \operatorname{tr}^{1/6}(\boldsymbol{P}^6) = 45^{1/3} \approx 3.5569.$$

Calculation of the Kleene star matrix gives

$$(\mu^{-1}\boldsymbol{P})^* = \begin{pmatrix} 1 & 675/\mu^5 & 378/\mu^4 & 189/\mu^4 & 3/\mu & 7/5 \\ 3/\mu & 1 & 1134/\mu^5 & 567/\mu^5 & 405/\mu^5 & 21/5\mu \\ 2/15 & 2\lambda/5\mu & 1 & 126/\lambda\mu^5 & 90/\lambda\mu^5 & 42/\lambda\mu^4 \\ 81/\mu^4 & 3/5 & 18/\mu^2 & 1 & 243/\mu^5 & 3/\mu \\ 675/\mu^5 & 225/\mu^4 & 14/5 & 7/5 & 1 & 945/\mu^5 \\ 8/15 & 8\lambda/5\mu & 6/\mu & 3/\mu & 72\lambda/5\mu^3 & 1 \end{pmatrix}.$$

Using the generating matrix $(\mu^{-1}\boldsymbol{P})^*$ we calculate the best differentiating vector of ratings:

$$\boldsymbol{x} = (3/\mu,\ 405/\mu^5,\ 90/\lambda\mu^5,\ 243/\mu^5,\ 1,\ 72\lambda/5\mu^3)^{\mathrm{T}} \approx$$
$$\approx (0.8434,\ 0.7114,\ 0.1125,\ 0.4268,\ 1.0000,\ 0.4498)^{\mathrm{T}}.$$

The obtained vector sets the order $A_5 > A_1 > A_2 > A_6 > A_4 > A_3$.

With the worst differentiating vector of weights $\boldsymbol{w}$ we have the weighted sum

$$\boldsymbol{R} = 1/9\lambda \boldsymbol{A}_1 + \boldsymbol{A}_2 + \lambda/2\boldsymbol{A}_3 + \lambda/5\boldsymbol{A}_4 =$$

$$= \begin{pmatrix} 1 & 4 & 3 & 1 & 3 & 4 \\ 5\lambda/2 & 1 & 7 & 3 & 3\lambda/2 & 7\lambda/2 \\ 2/3\lambda & 2\lambda/5 & 1 & 1/5 & \lambda/4 & \lambda/2 \\ 3\lambda/2 & 4\lambda/5 & 5 & 1 & \lambda & 5\lambda/2 \\ \lambda & 5 & 5 & 1 & 1 & 3 \\ 3\lambda/5 & 8\lambda/5 & 6 & 3 & \lambda & 1 \end{pmatrix}.$$

The matrix $\boldsymbol{R}$ has the spectral radius

$$\mu = \operatorname{tr} \boldsymbol{R} \oplus \cdots \oplus \operatorname{tr}^{1/6}(\boldsymbol{R}^6) = (75\lambda/2)^{1/3} \approx 3.7495.$$

The Kleene star matrix $(\mu^{-1}\boldsymbol{R})^*$ is equal to

$$\begin{pmatrix} 1 & 1125\lambda/2\mu^5 & 315\lambda/\mu^4 & 315\lambda/2\mu^4 & 225\lambda/2\mu^4 & 7/5 \\ 375\lambda^2/4\mu^4 & 1 & 1575\lambda^2/2\mu^5 & 1575\lambda^2/4\mu^5 & 1125\lambda^2/4\mu^5 & 525\lambda^2/4\mu^4 \\ 75\lambda^3/2\mu^5 & 15\lambda^2/\mu^4 & 1 & 21\lambda^2/5\mu^3 & 3\lambda^2/\mu^3 & 105\lambda^3/2\mu^5 \\ 225\lambda^2/4\mu^4 & 3/5 & 15\lambda/\mu^2 & 1 & 675\lambda^2/4\mu^5 & 5\lambda/2\mu \\ 1875\lambda^2/4\mu^5 & 375\lambda/2\mu^4 & 14/5 & 7/5 & 1 & 2625\lambda^2/4\mu^5 \\ 150\lambda^3/\mu^5 & 60\lambda^2/\mu^4 & 6/\mu & 3/\mu & 12\lambda^2/\mu^3 & 1 \end{pmatrix}.$$

The worst differentiating vector of ratings takes the form:

$$\boldsymbol{y} = (4\mu^5/1875\lambda^2,\ 2\mu^4/375\lambda,\ 5/14,\ 5/7,\ 1,\ 4\mu^5/2625\lambda^2)^{\mathrm{T}} \approx$$

$$\approx (0.8001,\ 0.7499,\ 0.3571,\ 0.7143,\ 1,\ 0.5715)^{\mathrm{T}}.$$

The order defined by this vector is the order $A_5 > A_1 > A_2 > A_4 > A_6 > A_3$.

Conclusion

Note that in [4], the order of alternatives obtained using the analytic hierarchy process is given by $A_1 > A_2 > A_5 > A_6 > A_4 > A_3$. If we compare it with the best log-Chebyshev solution, we can see that the difference in solutions is in the first three ranks, the last three ranks completely coincide. In the case of comparison with the results of the worst differentiating solution, the three most preferred and the three least preferred alternatives coincide, but there is a different order within the triples. The difference between solutions makes it somewhat difficult to choose one most preferable alternative, but allows one to recognize a group of three most preferable alternatives.

References

[1] Kolokoltsov V.N., Maslov V.P. Idempotent Analysis and Its Applications; Mathematics and Its Applications; Springer: Dordrecht, The Netherlands, 1997; Volume 401.

[2] Heidergott B., Olsder G. J., van der Woude J. Max Plus at Work. Princeton Series in Applied Mathematics. Princeton: Princeton Univ. Press, 2006. 226 p.

[3] Krivulin, N. Using tropical optimization techniques in bi-criteria decision problems. Comput. Manag. Sci. 2020, 17, 79–104.

[4] Muralidhar K., Santhanam R., Wilson R. L. Using the analytic hierarchy process for information system project selection // Information and Management. 1990. Vol. 18, N 2. P. 87–95.

[5] Saaty, T.L. The Analytic Hierarchy Process, 2nd ed.; RWS Publications: Pittsburgh, PA, USA, 1990

[6] Krivulin, N. Methods of tropical optimization in rating alternatives based on pairwise comparisons. In Operations Research Proceedings 2016; Fink, A., Fügenschuh, A., Geiger, M.J., Eds.; Springer: Cham, Switzerland, 2018; pp. 85–91.

[7] Krivulin N. Methods of tropical optimization in rating alternatives based on pairwise comparisons // Operations Research Proceedings 2016 / Ed. by A. Fink, A. Fugenschuh, M. J. Geiger. Cham: Springer, 2018. P. 85–91.

Nikolai Krivulin
Faculty of Mathematics and Mechanics
Saint Petersburg State University
Saint Petersburg, Russia
e-mail: nkk@math.spbu.ru

Alexey Prinkov
Faculty of Mathematics and Mechanics
Saint Petersburg State University
Saint Petersburg, Russia
e-mail: aprinkov@yahoo.com

On the computation of Abelian differential of the third kind

Mikhail Malykh and Leonid Sevastianov

Abstract. We consider the construction of the fundamental function and Abelian differentials of the third kind on a plane algebraic curve over the field of complex numbers that has no singular points. The algorithm for constructing differentials of the third kind is described in Weierstrass's Lectures. The article discusses its implementation in the Sage computer algebra system. The specificity of this algorithm, as well as the very concept of the differential of the third kind, implies the use of not only rational numbers, but also algebraic ones, even when the equation of the curve has integer coefficients. Sage has a built-in algebraic number field tool that allows implementing Weierstrass's algorithm almost verbatim. The simplest example of an elliptic curve shows that it requires too many resources, going far beyond the capabilities of an office computer. Then the symmetrization of the method is proposed and implemented, which solves the problem and allows significant economy of resources. The algorithm for constructing a differential of the third kind is used to find the value of the fundamental function according to the duality principle. Examples explored in the Sage system are provided.

Of all the known approaches to Abelian integrals, Weierstrass's approach was the most constructive. In Ref. [1], we tried to show that the normal form of representation of Abelian integrals proposed in the lectures gives solutions to a number of classical problems and its implementation in computer algebra systems would be very useful. The key problem on this way, both in the 19th century and now, is the construction of the fundamental function (Hauptfuktion) or, which is also due to the duality principle, the differential of the third kind (Art), the construction algorithm of which is described in the last chapter of Part 1 of the Weierstrass Lectures [2], published in 1902 by Hettner and Knoblauch. There are no examples of using the algorithm in the text.

A characteristic feature of Weierstrass' approach is the use of a large number of irrational numbers, the algorithm for determining which is either described in the text, or more or less obvious. The Sage system has a built-in implementation QQbar of the field of algebraic numbers, so in theory the algorithms from the

Lectures can be implemented as written. However, in practice, symbolic expressions containing a ten of numerical coefficients from the field of algebraic numbers QQbar are very difficult to manipulate. We decided to consider this direct implementation of the algorithms and these expressions themselves and evaluate the difficulties that arise.

Let polynomial f define an algebraic curve C of the order r on the projective plane xy over the field $\mathbb{C}$. Let for simplicity this curve have no singular points.

Definition. A differential of the form udx, $u \in \mathbb{C}(x,y)$ having no singular points is called a differential of the first kind. A differential of the form udx, $u \in \mathbb{C}(x,y)$ is called a differential of the third kind, if it has two singular points, namely, poles of the first order (x_1, y_1) and (x_2, y_2) with residues 1 and -1.

Problem 1. Given a polynomial $f \in \mathbb{Q}[x,y]$, find a non-constant rational function $u \in \overline{\mathbb{C}}(x,y)$ such that udx is a differential of the first kind.

The absence of finite singular points makes one seek the solution in the form

$$\frac{E(x,y)dx}{f_y(x,y)}, \quad E \in \mathbb{C}[x,y],$$

and the absence of singular points at infinity indicates the fact that the order of the polynomial E cannot exceed $r-3$. Since no limitations should be imposed on the coefficients of this polynomial, the set of differentials of the first kind has the dimension

$$p = \frac{(r-1)(r-2)}{2},$$

which is called a genus of the curve. For the basis of this space one can take differentials with the coefficients form the field $\mathbb{Q}$, rather than from its algebraic closure. Therefore, when constructing differentials of the first kind it is possible and necessary to work over the field $\mathbb{Q}$.

Algorithms for calculating a basis for the space of differentials of the first kind for planar curves, including those having singular points, have been proposed both in classical books and in present-day papers [3]. At present they are implemented in the systems Maple (AlgCurves, CASA) and Sage.

Problem 2. Given a indecomposable polynomial $f \in \mathbb{Q}[x,y]$, defining a projective curve C, and two points (x_1, y_1) and (x_2, y_2) on this curve, and $x_1, x_2, y_1, y_2 \in \overline{\mathbb{Q}}$. It is required to construct a non-constant rational function $u \in \mathbb{C}(x,y)$ such that udx is a differential of the third kind with the poles (x_1, y_1) and (x_2, y_2).

The addition to the differential of a linear combination of differentials of the first kind does not give rise to new singularities of change of residues, therefore, the solution of Problem 2 is defined to a linear combination of p differentials of the first kind.

The absence of finite singular points with $x \neq x_i$ makes one seek the solution in the form

$$\frac{E(x,y)dx}{(x-x_1)(x_2-x)f_y(x,y)}, \quad E \in \mathbb{C}[x,y],$$

and the absence of points at infinity indicates the fact that the order of the polynomial E cannot exceed $r-1$. Equation

$$f(x_i, y) = 0$$

beside the root $y = y_i$ has $r-1$ more roots; let us denote them as $y_i', \dots, y_i^{(r-1)}$. If there are no multiple roots among them, then the equations

$$E(x_i, y_i^{(j)}) = 0, \quad i = 1, 2,\ j = 1, \dots, r-1$$

ensure the absence of singularities at point, different from (x_1, y_1) and (x_2, y_2). The conditions for residues at these points give two more equations:

$$E(x_1, y_1) = (x_2 - x_1) f_y(x_1, y_1), \quad E(x_2, y_2) = (x_2 - x_1) f_y(x_2, y_2).$$

Thus, the solution to Problem 2 reduces to the solution of a system of linear equations with coefficients from QQbar, and the main difference of Problem 2 from Problem 1 is the necessity to extend the number field.

We wrote a directi realization of the described method in Sage and applied it to an elliptic curve

$$x^3 - y^3 + 2xy + x - 2y + 1 = 0.$$

The solution of Problem 2 led to six linear equations with six unknowns $c_0, \dots, c_5$. To solve systes of equations, Sage uses a standard function `solve`, which does not support the operation with algebraic numbers. Therefore, we proceeded to matrices over the field of algebraic numbers and tried to solve the system of linear equations by means of function `solve_right`. However, this function did not cope with this system in a reasonable amount of time.

Fortunately, the system of equations consists of two subsystems of the form

$$E(x_i, y_i^{(j)}; c_0, \dots) = b_{i,j}, \quad j = 1, 2, \dots r, \tag{1}$$

where $y_i^{(j)}$ is te set of roots of equation $f(x_i, y) = 0$ with respect to y. It can be symmetrized and its solution can be reduced to inverting matrices with rational coefficient. In the example considered, a visually graspable expression is obtained

```
( -0.9888519187910046?* x * y - y ^2 +
0.1254856073486862?* x - 0.4533976515164038?* y -
2.205569430400590?) * dx /((3* y ^2 - 2* x + 2) *( x - 1) * x)
```

Thus, such symmetrization is quite enough for efficient implementation of the method for constructing a differential of the third kind, proposed in Weierstrass's Lectures.

The next step in implementing algorithms, proposed in Weierstrass's Lectures, is the construction of the fundamental function. For this purpose, it is sufficient to construct a differential of the third kind with a movable pole. To execute symmetrization in this case, too, we intend to use a perfect tool — the package Symmetric Functions for Sage, which allows expressing a symmetric function from a ring $K[x_1, \dots, x_n]$ as a linear combination of elementary symmetric functions.

Acknowledgments. This work is supported by the Russian Science Foundation (grant no. 20-11-20257).

References

[1] M.D. Malykh; L.A. Sevastianov; Y. Yu, On symbolic integration of algebraic functions. *Journal of Symbolic Computation* **104**, 563–579 (2021).

[2] K. Weierstrass *Math. Werke.* Vol. 4. Mayer & Müller, Berlin, 1902.

[3] M. van Hoeij, An algorithm for computing an integral basis in an algebraic function field. *Journal of Symbolic Computation* **18**, 353–363 (1994).

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

e-mail: malykh_md@pfur.ru

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

e-mail: sevastianov_la@pfur.ru

Fourier series summation and A.N. Krylov convergence acceleration in CAS

Ksaverii Malyshev

Abstract. The summation of Fourier series in finite terms is considered. First at all, we want to present some results about testing standard instruments for calculating of infinite sums in modern CAS. They work over the field of complex numbers and, in the case of Fourier series, sometimes this lead to strange forms for symbolic representation of sums.

Then we want suggest an alternative approach to the summation of Fourier series, based on a method, proposed by A.N. Krylov for the acceleration of Fourier series convergence. We consider examples of Fourier series from mathematical physics related to the wave equation, and especially the Green's functions of a finite string. Sometimes, and for several Green's functions espessially this approach give zero expression instead of a fast convergence Fourier series. This means in our viewpoint that we find the summation of Fourier series in finite terms. In this case, it is supposed to use the field of real numbers. The advantages and difficulties of both approaches and their implementation in CAS are discussed.

References

[1] Krylov A.N., *O nekotoryh differencial'nyh uravneniyah matematicheskoj fiziki (in Russian)*, GITTL, Moscow-Leningrad, 1950.

[2] Adcock B., *Modified Fourier expansions: theory, construction and application*, Trinity Hall, University of Cambridge, 2010.

[3] Symbolic and numeric computing environment Maple, 2019. `https://www.maplesoft.com/`

Ksaverii Malyshev
Skobeltsyn Institute of Nuclear Physics, M.V. Lomonosov Moscow State University, Moscow, Russia

e-mail: `kmalyshev08102@mail.ru`

Fair division algorithms with a small number of queries

Andrei Malyutin

Abstract. We study the algorithmic complexity of fair division problems with a focus on minimizing the number of queries needed to find an approximate solution with desired precision. In a recent joint work with Alexandr Grebennikov, Xenia Isaeva, Mikhail Mikhailov, and Oleg Musin, we showed for several classes of fair division problems that under certain natural conditions on sets of preferences, a polylogarithmic number of queries with respect to the reciprocal of accuracy is sufficient. The present note extends these results (on the sufficiency of polylogarithmic number of queries) to the case of four or more tenants in the rental harmony problem with convex preference sets.

We study algorithmic aspects of the so-called fair division problems. A nice introduction to the subject is given in the book [RW98]. In this note, we discuss the following specific algorithmic geometry problem, the relation of which to the rental harmony problem (this is a type of fair division problems) is explained, e. g., in a recent paper [GIMMM].

1. Stating an algorithmic problem

Let $k \geq 2$ be a positive integer, let Δ_k be a $(k-1)$-dimensional regular simplex with edges of length 1 in $\mathbb{R}^{k-1}$, and let $v_1, \ldots, v_k$ be the vertices of Δ_k. For $j \in \{1, \ldots, k\}$, we denote the facet $\operatorname{Conv}(\{v_i\}_{i \neq j})$ of Δ_k, where $\operatorname{Conv}(X)$ stands for the convex hull of X, by F_j. (For the rental harmony problem, Δ_k corresponds to all representations of total price as a sum of k nonnegative numbers; and F_j is precisely the set of price distributions with zero price for the jth room.)

Assume that a collection of k subsets $P_1, \ldots, P_k$ of Δ_k is fixed such that

(P1) $\{P_1, \ldots, P_k\}$ is a covering of Δ_k, that is, $\bigcup_{i \in \{1,\ldots,k\}} P_i = \Delta_k$;

(P2) P_i contains F_i for each $i \in \{1, \ldots, k\}$;

This work was supported by RFBR, research project no. 20-01-00070.

(P3) P_i is convex for each $i \in \{1, \dots, k\}$;
(P4) P_i is closed for each $i \in \{1, \dots, k\}$.[1]

Assume that we have no description of the sets $P_1, \dots, P_k$, but we know that the sets have the listed properties and we can perform queries about these sets: if we choose an index $i \in \{1, \dots, k\}$ and a point $x \in \Delta_k$, we receive 'yes' if $x \in P_i$ and 'no' otherwise.

The Knaster–Kuratowski–Mazurkiewicz (KKM) lemma guarantees (due to the properties (P1), (P2), and (P4)) that the intersection $\bigcap_{i \in \{1,\dots,k\}} P_i$ is nonempty, so that there exists a point x in Δ_k such that $\operatorname{dist}(x, P_i) = 0$ for all $i \in \{1, \dots, k\}$. We say that such x in Δ_k is a *solution* for $\mathscr{P} = \{P_1, \dots, P_k\}$. We say that x in Δ_k is an *ε-solution*, $\varepsilon \geq 0$, for $\mathscr{P}$ if $\operatorname{dist}(x, P_i) \leq \varepsilon$ for all $i \in \{1, \dots, k\}$.[2]

Our goal is to construct an algorithmic procedure that, given a collection $\{P_1, \dots, P_k\}$ (having properties (P1)–(P4)) and an 'accuracy constant' $\varepsilon > 0$ finds an ε-solution using the smallest possible number of queries.

2. The main result

It is known that ε-nets allow us to find ε-solutions with $O(1/\varepsilon)^{k-1}$ queries. In the case $k = 2$, we can use binary search to find an ε-solution in the interval Δ_2 with $O(\log(1/\varepsilon))$ queries. Theorem 5.2 in [GIMMM] implies that in the case $k = 3$, an ε-solution can be found with $O(\log(1/\varepsilon))^2$ queries. A natural conjecture arises that an ε-solution can be found with $O(\log(1/\varepsilon))^{k-1}$ queries. The main result of the present note confirms this conjecture for $k = 4$.

Theorem 1. *In the case $k = 4$, an ε-solution for convex P_i can be found with $O(\log(1/\varepsilon))^3$ queries.*

Theorem 1 implies (modulo results of [GIMMM] and using terminology introduced there) that, for the rental harmony problem with 4 tenants having convex preference sets, we can find an ε-fair division point in binary mode with $O(\log(1/\varepsilon))^3$ queries.

3. Basic idea of the algorithm

The description of our algorithm is rather cumbersome, and before proceeding to it, we will outline its core idea. This idea seems to work for an arbitrary dimension, but here we restrict ourselves to the case of $k = 4$. Let us fix one of the facets F_1, F_2, F_3, F_4 (say, F_4) and study the sections of our Δ_4 with hyperplanes parallel to F_4. These sections form a bundle $(T_\theta)_{\theta \in [0,1]}$ of regular triangles, where θ is the diameter of T_θ; we have $T_0 = v_4$ and $T_1 = F_4$. The first key observation we need

[1] In fact, we can carry out our constructions without condition (P4), but we introduce it for convenience, in order not to repeatedly mention the transition to closures in what follows.
[2] We remark that an ε-solution is not necessarily located close to a solution. It is easy to construct an example when the distance between an ε-solution and the solution closest to it exceeds 100ε.

is that if P_1, P_2, P_3 do not cover T_θ for some θ (so that $T_\theta \setminus (P_1 \cup P_2 \cup P_3)$ is nonempty) then T_θ contains a unique '*inscribed circle*' S_θ that touches each of P_1, P_2, and P_3 and has no points of $P_1 \cup P_2 \cup P_3$ inside. The center of S_θ is an r_θ-solution, where r_θ is the radius of S_θ. Thus, if given an $\varepsilon > 0$ we find some $\theta \in [0,1]$ such that $T_\theta \setminus (P_1 \cup P_2 \cup P_3)$ is nonempty and $r_\theta \leq \varepsilon$, then the center of S_θ will be the desired ε-solution. Observe that, due to convexity arguments, if the set $\mathscr{I}$ of those θ for which P_1, P_2, P_3 do not cover T_θ is nonempty, then this $\mathscr{I}$ is a half-open subinterval in $[0,1]$ of the form $(\theta', 1]$, and the radii r_θ form a continuous monotone function on this subinterval $\mathscr{I}$. Using this, we can try to find θ with a small radius $r_\theta \leq \varepsilon$ via binary search. Take $\theta_1 = 1/2$. If $1/2$ is not in $\mathscr{I}$, then put $\theta_2 = 3/4$, and if $1/2$ is in $\mathscr{I}$ and $r_{1/2} > \varepsilon$, then put $\theta_2 = 1/4$, and so on. For example, if the set $\mathscr{I}$ is empty or of length less than ε, then at the step $m = \log_2\lceil 1/\varepsilon \rceil$ we get $\theta_m = 1 - 1/2^m \geq 1 - \varepsilon$ and any point in the nonempty (by the KKM lemma) set $T_{\theta_m} \cap P_1 \cap P_2 \cap P_3$ is an ε-solution (because $F_4 \subset P_4$ is close enough).

A difficulty arising when implementing the described idea as an algorithmic procedure is that a monotone function can have 'jumps'. This issue is resolvable due to the fact that the function r_θ is convex in addition. Another difficulty is the calculation of inscribed circles.

3.1. Inscribed antitriangles

In order to simplify computations, instead of finding (approximately) inscribed circles S_θ for triangles T_θ, we introduce and calculate (approximately) *inscribed antitriangles*. By an *antitriangle* in a triangle T_θ (in the above notation) we mean any regular triangle contained in T_θ that is related to T_θ by a negative homothetic transformation. An antitriangle A in T_θ is *inscribed* if the intersection of A with the union $P_1 \cup P_2 \cup P_3$ is the set of vertices of A. It can be shown that if $T_\theta \setminus (P_1 \cup P_2 \cup P_3)$ is nonempty then there exists a unique inscribed antitriangle A_θ for T_θ. Observe that if $T_\theta \setminus (P_1 \cup P_2 \cup P_3)$ is nonempty, then the center of the inscribed antitriangle A_θ is a $(\mathrm{Diam}\,(A_\theta)\,/\sqrt{3})$-solution, where $\mathrm{Diam}\,(A_\theta)$ is the diameter of A_θ, while any point in A_θ is a $\mathrm{Diam}\,(A_\theta)$-solution. Similar to the approach with inscribed circles, the diameters $\mathrm{Diam}\,(A_\theta)$ form a continuous monotone convex function on $\mathscr{I}$. Using this, we can try to find θ with a small $\mathrm{Diam}\,(A_\theta)$ via binary search.

4. Procedure for finding inscribed antitriangles (PFIA)

Now we describe a computational procedure that, given an arbitrary $\theta \in (0,1]$, operates in the triangle T_θ and calculates, with a prescribed precision, the size of the inscribed antitriangle A_θ and its position (if it is large enough). The input of the procedure is the 'coordinate' θ and a 'precision constant' $\delta > 0$. The outputs of the procedure are:

- A (nonnegative real) number d_θ such that $|d_\theta - \mathrm{Diam}\,(A_\theta)| \leq \delta$ (if A_θ is undefined, we formally set $\mathrm{Diam}\,(A_\theta) = 0$ so that $d_\theta \leq \delta$ in this case).

- A point x_θ in T_θ such that the metric ball $B_{d_\theta+\delta}(x_\theta)$ of radius $d_\theta+\delta$ centered at x_θ intersects P_1, P_2, and P_3. Besides, $B_{d_\theta+\delta}(x_\theta)$ intersects P_4 whenever $\mathrm{Diam}\,(A_\theta) > \delta$.

In this procedure, we fix one of the facets F_1, F_2, F_3 (say, F_3) and regard T_θ as a bundle of closed segments parallel to the edge $T_\theta \cap F_3$. For this bundle, we use the notation $(I_\alpha)_{\alpha\in[0,\theta]}$, where I_α is the segment of length α (so that $I_\theta = T_\theta \cap F_3$ and I_0 is the opposite vertex of T_θ). For each $\alpha \in [0,\theta]$, the segment I_α is isometric to the segment $[0,\alpha]$. In the following description, when α is fixed we identify I_α with $[0,\alpha]$ via the isometry sending the endpoint $I_\alpha \cap F_1$ to $\{0\}$ in $[0,\alpha]$.

If $T_\theta \setminus (P_1 \cup P_2 \cup P_3)$ is nonempty and the inscribed antitriangle A_θ exists, then there is a unique $\eta \in (0,\theta)$ such that I_η contains an edge of A_θ. In this case we use the notation $E(\theta) = \eta$. If $T_\theta \setminus (P_1 \cup P_2 \cup P_3)$ is empty, we set $E(\theta) = \theta$. The procedure uses several levels of binary searches, the upper level goes through the interval $[0,\theta]$ and study segments I_α of $(I_\alpha)_{\alpha\in[0,\theta]}$, which can be regarded as aiming to 'find' (approximately) the segment $I_{E(\theta)}$.

We set $a_1 = 0$ and $b_1 = \theta$ and start an iterative process with intervals $[a_i, b_i]$ in $[0,\theta]$ such that $[a_i, b_i]$ contains $E(\theta)$ if $\mathrm{Diam}\,(A_\theta)$ is large enough. Given a_i and b_i such that $0 \le a_i < b_i \le \theta$, the ith iteration looks as follows. We set $c_i := (a_i + b_i)/2$ and operate in the segment I_{c_i} (which is parametrized as $[0, c_i]$ by the above convention). In $m := \lceil \log_2(9c_i/\delta)\rceil \le \lceil \log_2(1/\delta)\rceil + 4$ queries we can find in $I_{c_i} = [0, c_i]$ a half-open subinterval of the form $[p\delta', p\delta' + \delta')$, where p is an integer and $\delta' = c_i/2^m \le \delta/9$, such that

$$[0, p\delta'] \subset (I_{c_i} \cap P_1) \subset [0, p\delta' + \delta').$$

Another m queries allow us to find $q \in \mathbb{Z}$ such that $(q\delta', q\delta' + \delta']$ contains the endpoint g of $I_{c_i} \cap P_2$ such that $[g, c_i] = I_{c_i} \cap P_2$. We have three cases:

$q < p$, which means that $P_1 \cup P_2$ contains I_{c_i} and $c_i < E(\theta)$. In this case, we set $[a_{i+1}, b_{i+1}] := [c_i, b_i]$ and pass to the next iteration.

$q = p$, which means that either $P_1 \cup P_2$ contains I_{c_i} or the interval $I_{c_i} \setminus (P_1 \cup P_2)$ has length at most δ. In the case $q = p$, we also set $[a_{i+1}, b_{i+1}] := [c_i, b_i]$ for the next iteration, even though it is possible that $E(\theta) = c_i$. In fact, if $q = p$, then $E(\theta)$ can take any position in $(0, c_i)$, but we see that if $q = p$ and $E(\theta) \le c_i$, then the diameter of A_θ is at most δ, which is less than our 'level of visibility' limit.

$q > p$, in this case we see that the length of $I_{c_i} \setminus (P_1 \cup P_2)$ is greater than $(q-p-1)\delta'$ and lesser than $(q-p+1)\delta'$. In the case $q > p$, we do additional computations.

Additional computations for the case $q > p$ are as follows. If the subsegment $[p\delta', q\delta' + \delta']$ of I_{c_i} is an edge of an antitriangle contained in T_θ, we denote the opposite vertex of this antitriangle by w. If the subsegment $[p\delta' + \delta', q\delta']$ of I_{c_i} is an edge of an antitriangle contained in T_θ, we denote the opposite vertex of this antitriangle by v. If any of v and w is defined, we perform a query whether P_3 contains it. Then, for the case $q > p$, we introduce three subcases:

(L) either v is not defined or $v \in P_3$. In this case, we have $E(\theta) < c_i$, and we set $[a_{i+1}, b_{i+1}] := [a_i, c_i]$ (and pass to the next iteration).
(R) w is defined and $w \notin P_3$. In this case, $E(\theta) > c_i$. We set $[a_{i+1}, b_{i+1}] := [c_i, b_i]$.
(+) v is defined and $v \notin P_3$ while w is either not defined or $w \in P_3$. In this case, we have $|\mathrm{Diam}\,(A_\theta) - (q-p)\delta'| \leq \delta'$, and we stop our procedure with setting $d_\theta = (q-p)\delta'$ and x_θ to be the center of the antitriangle with edge $[(p+1)\delta', q\delta']$ (or just set x_θ to be any point of this edge).

This completes the description of the iterative step.

We continue the iterative process either until subcase (+) happens or stop at step $2\lceil \log_2(1/\delta)\rceil + 10$. If subcase (+) happens, the output of the procedure is described above. If we stop at the step $t = 2\lceil \log_2(1/\delta)\rceil + 10$ with no (+) subcase, the situation splits in two following subcases.

- The subcase with $a_t > \theta - \delta/2$. It can be shown that the only way to get $a_t > \theta - \delta/2$ is to have 'short' interval $I_{\theta-\delta} \setminus (P_1 \cup P_2)$ of length less than $\delta + 2\delta/9$. In this case we have $\mathrm{Diam}\,(A_\theta) < 2\delta$ and we can set $d_\theta = \delta$. The point x_θ can be chosen in $I_{\theta-\delta}$ in an obvious way.
- If $a_t \leq \theta - \delta/2$, we study the segment I_{a_t}. Clearly, $2\lceil \log_2(1/\delta)\rceil + 10$ queries is enough to find h such that

$$|h - \mathrm{Diam}\,(I_{a_t} \setminus (P_1 \cup P_2))\,| < \delta/9$$

  and $x \in I_{a_t}$ such that x $(\delta/9)$-approximates the center of that of the two intervals $I_{a_t} \setminus (P_1 \cup P_2)$ and $I_{a_t} \cap P_1 \cap P_2$ which is nonempty. Then we set $d_\theta := h + \delta/2$ and $x_\theta := x$ and quit the procedure.[3]

5. Description of the algorithm (of finding an ε-solution)

Now we turn to the description of our algorithm that, given an 'accuracy constant' ε and a collection $\mathscr{P} = \{P_1, P_2, P_3, P_4\}$ of subsets with properties (P1)–(P4) in Δ_4, following the basic idea described above, and using the procedure described above (PFIA), finds an ε-solution for this $\mathscr{P}$.

Algorithm starts with applying PFIA to the triangle $T_{1-\varepsilon}$ (see notation in Sec. 3). Let the input accuracy constant δ for PFIA be $\varepsilon/9$.

If PFIA says that $d_{1-\varepsilon} \leq \varepsilon - \delta$, which means that the set $T_{1-\varepsilon} \setminus (P_1 \cup P_2 \cup P_3)$ is either empty or 'thin enough', then the point $x_{1-\varepsilon}$ (this point is in the output of PFIA; see the description of PFIA) is an ε-solution because the metric ball $B_\varepsilon(x_{1-\varepsilon})$ of radius ε centered at $x_{1-\varepsilon}$ intersects P_4 (which contains F_4) and P_1, P_2, and P_3 as well (because $B_{d_{1-\varepsilon}+\delta}(x_{1-\varepsilon})$ by construction of PFIA intersects

---

[3] In order to prove that the assigned values of d_θ and x_θ indeed have the properties declared for the output, we check several various cases and use properties of convex sets. One of the key points of our proof is the fact that corresponding endpoints of the intervals $I_{a_t} \setminus (P_1 \cup P_2)$ and $I_{b_t} \setminus (P_1 \cup P_2)$ are located at a small distance from each other. This fact follows from the conditions $a_t \leq \theta - \delta/2$ and $b_t - a_t \leq \delta^2/100$ and can be proved by analogy with the simple observation given in Sec. 5.2.

P_1, P_2, and P_3 while $d_{1-\varepsilon} + \delta \le \varepsilon - \delta + \delta = \varepsilon$ so that $B_{d_{1-\varepsilon}+\delta}(x_{1-\varepsilon}) \subset B_\varepsilon(x_{1-\varepsilon}))$. Then the algorithm stops.

Otherwise, if $d_{1-\varepsilon} > \varepsilon - \delta$, the algorithm goes into an iterative process with intervals $[a_i, b_i]$ in $[0,1]$ such that $d_{a_i} \le \delta$ and $d_{b_i} > \varepsilon - \delta$ (in the present settings we have $\varepsilon - \delta = 8\varepsilon/9$). Having $d_{1-\varepsilon} > \varepsilon - \delta$, we set $[a_1, b_1] = [2\delta, 1-\varepsilon]$. Each subsequent iteration, being given $[a_i, b_i]$ with $d_{a_i} \le \delta$ and $d_{b_i} > \varepsilon - \delta$, we set $c_i = (a_i + b_i)/2$ and apply PFIA to the triangle T_{c_i} obtaining d_{c_i} and x_{c_i} as its output.

- If $d_{c_i} \le \delta$, we move on to the next iteration with $[a_{i+1}, b_{i+1}] := [c_i, b_i]$.
- If $d_{c_i} > \varepsilon - \delta$, we move on to the next iteration with $[a_{i+1}, b_{i+1}] := [a_i, c_i]$.
- If $d_{c_i} \in (\delta, \varepsilon - \delta]$, then $\mathrm{Diam}\,(A_{c_i}) \in (0, \varepsilon]$ (because $|d_\theta - \mathrm{Diam}\,(A_\theta)\,| \le \delta$) and x_{c_i} is an ε-solution for $\mathscr{P}$ (by construction of PFIA).

5.1. Estimating the number of queries

Observe that $\mathrm{Diam}\,(A_t)$, $t \in [0,1]$, is a convex nonnegative function. In particular, for any a and b in $[0,1]$ such that $0 \le a < b \le 1$, we have (cf. Sec. 5.2)

$$\frac{\mathrm{Diam}\,(A_b) - \mathrm{Diam}\,(A_a)}{b-a} \le \frac{\mathrm{Diam}\,(A_1) - \mathrm{Diam}\,(A_a)}{1-a}.$$

Suppose that the upper level iterative process in our algorithm arrives at step i. Since $\mathrm{Diam}\,(A_1) \le 1/2$, $a_i < b_i \le 1 - \varepsilon$, $|d_\theta - \mathrm{Diam}\,(A_\theta)\,| \le \delta$, and $\mathrm{Diam}\,(A_{a_i}) \le d_{a_i} + \delta \le 2\delta$ in our case, it follows that

$$d_{b_i} \le \frac{b_i - a_i}{2\varepsilon} + 3\delta.$$

Since $\varepsilon - \delta < d_{b_i}$ and $\delta = \varepsilon/9$, this implies that

$$\varepsilon^2 < b_i - a_i.$$

Since $b_i - a_i \le 2^{1-i}$, it follows that a necessary conditions for the transition to the ith iteration is the validity of the inequality

$$i < \log_2(2/\varepsilon^2) = 1 + 2\log_2(1/\varepsilon).$$

Therefore, since we refer to PFIA before iterations only once, our algorithm arrives at an ε-solution by calling procedure PFIA at most $1 + 2\log_2(1/\varepsilon)$ times. Each iteration of PFIA requires at most $(2\lceil\log_2(1/\varepsilon)\rceil + 10)^2$ queries, so the total search takes at most $(2\lceil\log_2(1/\varepsilon)\rceil + 10)^3$ ones.

5.2. An observation concerning convex/concave functions

Let $f\colon [0,1] \to \mathbb{R}$ be a nonnegative concave function with domain $[0,1]$, and let a and b be numbers in $[0,1]$ such that $0 \le a < b \le 1$. Then

$$\frac{f(b) - f(a)}{b-a} \le \frac{f(b)}{b} \quad \text{and} \quad \frac{f(a) - f(b)}{b-a} \le \frac{f(a)}{1-a}.$$

In particular, if $f(a)$ and $f(b)$ are in $[0,1]$ and for some $\delta > 0$ we have $\delta \le a < b \le 1 - \delta$ and $b - a \le \delta^2$, then

$$|f(b) - f(a)| \le \delta.$$

References

[A18] Asada, M., Frick, F., Pisharody, V., Polevy, M., Stoner, D., Tsang, L., Wellner, Z.: Fair division and generalizations of Sperner- and KKM-type results. SIAM J. Discrete Math. **32**, 591–610 (2018)

[AZ14] Azrieli, Y., Shmaya, E.: Rental harmony with roommates. Journal of Mathematical Economics **46**, 303–310 (2014)

[Ba89] Bapat, R. B.: A constructive proof of a permutation-based generalization of Sperner's lemma. Mathematical Programming **44**, 113–120 (1989)

[DQS12] Deng, X., Qi, Q., Saberi, A.: Algorithmic Solutions for Envy-Free Cake Cutting. Operations Research **60**, 1461–1476 (2012)

[DS61] Dubins, L. E., Spanier, E. H.: How to cut a cake fairly. Amer. Math. Monthly **68**, 1–17 (1961)

[FHEM19] Frick, F., Houston-Edwards, K., Meunier, F.: Achieving rental harmony with a secretive roommate. Amer. Math. Monthly **126**(1), 18–32 (2019)

[Ga84] Gale, D.: Equilibrium in a discrete exchange economy with money. International Journal of Game Theory **13**, 61–64 (1984)

[GIMMM] Grebennikov, A., Isaeva, X., Malyutin, A. V., Mikhailov, M., Musin, O. R.: Logarithmic algorithms for fair division problems (2021). `arXiv:2112.13622`

[KKM29] Knaster, B., Kuratowski C., Mazurkiewicz S.: Ein Beweis des Fixpunktsatzes für n-dimensionale Simplexe. Fundamenta Mathematicae **14**, 132–137 (1929)

[Mu14] Musin, O. R.: Around Sperner's lemma (2014). `arXiv:1405.7513`

[Mu16] Musin, O. R.: Homotopy invariants of covers and KKM-type lemmas. Algebr. Geom. Topol. **16**(3), 1799–1812 (2016)

[Mu17] Musin, O. R.: KKM type theorems with boundary conditions. J. Fixed Point Theory Appl. **19**(3), 2037–2049 (2017)

[RW98] Robertson, J., Webb, W.: Cake-Cutting Algorithms: Be Fair if You Can (1st ed.). A K Peters/CRC Press, Nattick, MA (1998)

[Ste49] Steinhaus, H.: Sur las division pragmatique. Econometrica **17**, 315–319 (1949)

[Str80] Stromquist, W.: How to cut a cake fairly. Amer. Math. Monthly **87**, 640–644 (1980)

[Su99] Su, F. E.: Rental harmony: Sperner's lemma in fair division. *Amer. Math. Monthly* **106**(10), 930–942 (1999)

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

Computing the dimensions of the components of tropical prevarieties

Farid Mikhailov

Abstract. The main goal of this work is the study of tropical recurrent sequences determined by various relations. For a set of tropical recurrent sequences described by tropical relations, D. Grigoriev put forward a hypothesis of stabilization of the maximum dimensions of the components of tropical prevarieties. This hypothesis has not been proven yet. As part of this work, for various recurrent sequences, the appropriate tropical prevarieties were examined using the gfan package in order to check Grigoriev's hypotises. The validity of such a hypothesis would make it possible to calculate the corresponding dimensions for a recurrent sequence for an arbitrary length.

Introduction

As part of this work, for various tropical recurrent relations, the corresponding tropical prevarieties were studied using the Gfan package in order to check the Grigoriev hypothesis about the stabilization of the maximum dimensions of the components, i.e the existence of a tropical analogue of the Hilbert polynomial. This hypothesis has not been proven yet. As part of this work, for various recurrent sequences, the appropriate tropical prevarieties were examined using the gfan package in order to check Grigoriev's hypotises.

In this work, the dimensions of the space of sequences are calculated in the cases of various recurrent relations. According to the calculated dimensions, the increase rate of the space of sequences relative to the number of elements in finite tropical sequences was revealed. Based on this regularity, hypotheses were made about the value of tropical entropy for various tropical recurrence relations. The calculations were made in the gfan package developed in 2005 by A. Jensen.

Gfan is a software package for calculating Gröbner fans and tropical varieties, developed in 2005 by A. Jensen, based on the algorithms in his dissertation [2]. The gfan package allows computing Gröbner bases, Gröbner fans, tropical prevarieties, varieties by given polynomials, and other objects of tropical geometry and the theory of Gröbner bases. It is currently the most powerful software tool for such calculations. Gfan is distributed as a standard Linux package and is part of the Debian distribution.

1. Basic objects of tropical math

Basic object of study is the *tropical semiring* $(\mathbb{R}\cup\{-\infty\},\oplus,\otimes)$. If T is an ordered semi-group then T is a tropical semi-ring with inherited operations $\oplus := max$, $\otimes := +$. As a set this is just the real numbers $\mathbb{R}$, together with an extra element $-\infty$. In this semiring, the basic arithmetic operations of addition and multiplication of real numbers are redefined as follows:

$$x \oplus y := \max(x, y) \quad \text{and} \quad x \otimes y := x + y.$$

Many of the familiar axioms of arithmetic remain valid in tropical mathematics. For instance, both addition and multiplication are commutative. These two arithmetic operations are also associative, and the times operator takes $\otimes$ precedence when plus $\oplus$ and times $\otimes$ occur in the same expression. The distributive law holds for tropical addition and multiplication. [4]

Both arithmetic operations have an identity element. Minus infinity is the identity element for addition and zero is the identity element for multiplication. An important difference between the tropical semiring and classical math is that tropical addition is idempotent $x \oplus x = x$.

Let $x_1, \ldots, x_n$ be variables which represent elements in the tropical semiring $(\mathbb{R}\cup\{-\infty\},\oplus,\otimes)$. By commutativity, we can sort the product and write tropical monomial in the usual notation, with the variables raised to exponents:

$$q(x_1, \ldots, x_n) = a \otimes x_1^{i_1} \otimes \cdots \otimes x_n^{i_n}.$$

A monomial represents a function from $\mathbb{R}^n$ to $\mathbb{R}$. When evaluating this function in classical arithmetic, what we get is a linear function:

$$q(x_1, \ldots, x_n) = a + i_1 \cdot x_1 + \cdots + i_n \cdot x_n.$$

A *tropical polynomial* is a finite linear combination of tropical monomials:

$$p(x_1, \ldots, x_n) = \bigotimes_j \left(a_j \otimes x_1^{i_{j_1}} \otimes \cdots \otimes x_n^{i_{j_n}}\right).$$

Here the coefficients a_j are real numbers and the exponents $i_{j_1}, \ldots, i_{j_n}$ are integers. Every tropical polynomial represents a function $\mathbb{R}^n \to \mathbb{R}$. When evaluating this function in classical arithmetic, what we get is the maximum of a finite collection of linear functions, namely

$$p(x_1, \ldots, x_n) = \max_j \left(a_j + i_{j_1} \cdot x_1 + \cdots + i_{j_n} \cdot x_n\right).$$

Definition 1. $x = (x_1, \ldots, x_n)$ is a *tropical zero* of p if maximum $\max_j q_j$ is attained for at least two different values of j.

Let some vector $w \in \mathbb{R}^n$ be given. We will use it as weight vector of some monomial ordering. And in this case, we allow negative values of the weigths. The initial form $\text{in}_w(f)$ of a polynomial f is the highest monomials of this polynomial when the degrees of monomials are weighted by the vector w.For example, if $g = x + 2y + z + 1$, then $\text{in}_{(0,0,1)}(g) = z$ and $\text{in}_{(0,0,-1)}(g) = x + 2y + 1$.The highest monomials at some weight vectors may have more than one. This is part of the description of a tropical hypersurface.

Definition 2. *Tropical hypersurface* of the polynomial f is the set

$$\mathcal{T}(f) = \{w \in \mathbb{R}^b : \text{in}_w(f) \text{ is not monomial}\}.$$

The tropical hypersurface is described in the same order space as the weight space. It is easy to see that if the weight vectors differ by a constant factor, then the weight orders are the same. That is, the membership of one point in the space of a tropical hypersurface entails the membership of the ray on which this point lies.

The connection between the concept of a tropical hypersurface and tropical mathematics lies in the process of tropicalization. Tropicalization is the transition from objects of classical mathematics to objects of tropical mathematics, which is carried out as follows: classical addition, multiplication and exponentiation are replaced by their tropical counterparts, the coefficients at monomials are assumed to be equal to zero.

Definition 3. *Tropical prevariety* of a system of polynomials $f_1, \ldots, f_n$ is the finite intersection of tropical hypersurfaces

$$\mathcal{T}(f_1) \cap \cdots \cap \mathcal{T}(f_n).$$

2. Tropical recurrent sequences

A classical linear recurrent sequence $\{z_j\}_{j\in\mathbb{Z}}$ satisfies conditions $\sum_{0\le i\le n} a_i z_{i+k} = 0, k \in \mathbb{Z}, a_0 \ne 0, a_n \ne 0$. A remarkable property of classical linear recurrent sequences is as follows: since the last coefficient a_n is not equal to zero, then if you calculate all z up to z_i, you can uniquely calculate z_{i+1} by substituting the corresponding k into the formula. This property is satisfied, since in classical arithmetic there are elements inverse in addition.

Definition 4. $y = y_i \in (\mathbb{R} \cup \{-\infty\})_{j\in\mathbb{Z}}$ is a *tropical recurrent sequence* if it satisfies conditions

$$\max_{0\le i\le n}(a_i + y_{k+i}), \quad k \in \mathbb{Z}, \quad a_0 > -\infty, a_n > -\infty. \tag{1}$$

The fulfillment of this condition means reaching the maximum in two or more tropical terms $a_i + y_{k+i}$.

The main difference between tropical recurrent sequences and classical ones is that each subsequent term, knowing the previous ones, is not always uniquely determined. Tropical recurrent sequences can be either periodic or non-periodic.

A sequence y is called periodic if $\exists d > 0$ such that $y_i - d_{i \in \mathbb{Z}}$ satisfies the tropical recurrence conditions 1.

Periodic recurrent sequences are in a sense trivial, since they correspond to classical recurrent sequences. The presence of non-periodic sequences is a tropical effect, and it is this presence that is the reason for the increase in the number of recurrent sequences with their length. To define tropical entropy, we introduce the concept of finite tropical recurrent sequences.

$y = (y_0, \dots, y_s) \in (\mathbb{R} \cup \{-\infty\})^{s+1}$ is a *finite tropical recurrent sequence* if it satisfies conditions

$$\max_{0 \le i \le n} (a_i + y_{k+i}), \quad k \in \{0, 1, \dots, s - n\}, \quad a_0 > -\infty, a_n > -\infty.$$

Definition 5. Denote by $D_s := D_s(a) \in (\mathbb{R} \cup \{-\infty\})^{s+1}$ the set of sequences satisfying vector a, and denote by $d_s := \dim D_s$. *Tropical entropy* is the limit $H(a) := \lim\limits_{s \to \infty} \frac{d_s}{s}$.

In the paper [1] D. Grigoriev proved the existence of entropy, as well as some properties.

3. Computing of tropical prevarieties corresponding to tropical recurrent sequences

Since the tropical entropy is a limit, in this paper reasonable hypotheses are given, what it can be equal to. To calculate the hypothetical tropical entropy, the vector a is associated with a system of $n - s + 1$ linear tropical equations with $s + 1$ unknowns, then the tropical prevariety of the system of equations are calculated. The gfan package is used to compute tropical prevarieties. The GFAN package computes tropical prevarieties only for polynomials with zero coefficients. For non-zero coefficients, a parametrization is introduced, which is discussed in detail in the GFAN manual [3] when calculating tropical curves.

From the computed tropical prevariety, one can find d_s. With a series of calculations with different s, you can find a pattern of growth in dimension and draw a conclusion about the hypothetical tropical entropy.

Using linear transformations, the vector $a = (a_0, \dots, a_n)$ can be associated with the vector $b = (0, b_1, \dots, b_{n-1}, 0)$. It is technically easier to consider cases in which $a_0 = 0$ and $a_n = 0$. The calculations were done for all such vectors of length n=3, presented in Table 1.

Conclusion

Computations of tropical prevarieties are performed to study the asymptotics of d_s and the conduct of the tropical entropy for various cases of a vector a of length $n = 3$. All hypothetical values of tropical entropy satisfy the properties proved in [1]. As a continuation of this work, it is proposed to do the following:

1. Computing of tropical prevarieties corresponding to tropical recurrent sequences of vectors of greater length.
2. Computing of tropical prevarieties for systems of non-recurrent equations.
3. Development of an interface for tropical computing.

$a\backslash s$	d_5	d_6	d_7	d_8	d_9	d_{10}	d_{11}	d_{12}	d_{13}	d_{14}	d_{15}	d_{16}	d_{17}	d_{18}	H(a)
(0,0,0,0)	4	4	4	5	6	6	6	7	8	8	8	9	10	10	1/2
(0,1,-1,0)	4	5	5	6	6	7	7	8	8	9	9	10	10	11	1/2
(0,-1,-1,0)	3	4	5	5	5	5	5	6	7	7	7	7	7	8	1/3
(0,1,2,0)	4	4	5	5	5	6	6	6	7	7	7	8	8	8	1/3
(0,-1,-2,0)	4	5	5	5	6	6	6	7	7	7	8	8	8	9	1/3
(0,-1,-3,0)	3	4	4	4	5	5	5	6	6	6	7	7	7	8	1/3
(0,-2,-3,0)	3	4	5	5	5	5	5	6	7	7	7	7	7	8	1/3
(0,-1,$-\infty$,0)	3	4	4	4	5	5	5	6	6	6	7	7	7	8	1/3
(0,0,$-\infty$,0)	3	3	4	4	4	4	5	5	5	6	6	6	6	7	2/7
(0,1,3,0)	4	4	4	4	5	5	5	5	6	6	6	6	7	7	1/4
(0,-1,2,0)	4	4	4	4	5	5	5	5	6	6	6	6	7	7	1/4
(0,1,-2,0)	3	4	4	4	4	5	5	5	5	6	6	6	6	7	1/4
(0,-1,0,0)	4	4	5	5	5	5	6	6	6	6	7	7	7	7	1/4
(0,1,0,0)	4	4	4	4	5	5	5	5	6	6	6	6	7	7	1/4
(0,1,$-\infty$,0)	3	4	4	4	4	5	5	5	5	6	6	6	6	7	1/4
(0,1,1,0)	3	3	3	3	3	3	3	3	3	3	3	3	3	3	0
(0,2,3,0)	3	3	3	3	3	3	3	3	3	3	3	3	3	3	0
(0,$-\infty,-\infty$,0)	3	3	3	3	3	3	3	3	3	3	3	3	3	3	0

TABLE 1. Hypothetical tropical entropy for $n = 3$

References

[1] Dima Grigoriev, *Tropical recurrent sequences*. CNRS, Math´ematique, Universit´e de Lille, Villeneuve d'Ascq, 59655, France, 2020, available at `https://logic.pdmi.ras.ru/~grigorev/pub/tropical_recurrent_revised.pdf`.

[2] Anders Nedergaard Jensen, *Algorithmic Aspects of Gröbner Fans and Tropical Varieties*. Department of Mathematical Science, Faculty of Science, University of Aarhus, 2007, available at `https://data.math.au.dk/publications/phd/2007/imf-phd-2007-anj.pdf`.

[3] Anders Nedergaard Jensen, *Gfan version 0.6: A User's Manual*. Department of Mathematical Science, Faculty of Science, University of Aarhus, 2017, available at `https://math.au.dk/~jensen/software/gfan/gfanmanual0.6.pdf`.

[4] Maclagan D., Sturmfels B, *Introduction to Tropical Geometry*, Providence: American Mathematical Society, 2015.

Farid Mikhailov
Department of Algorithmic Mathematics
Saint Petersburg Electrotechnical University "LETI"
Saint-Petersburg, Country
e-mail: mifa_98@mail.ru

Three-body dynamics: Agekian-Anosova region D

Aleksandr Mylläri and Tatiana Mylläri

Abstract. We discuss Agekian-Anosova homology region D and its impact on the studies of three-body dynamics.

Since it is impossible to obtain a general analytical solution to the three-body problem, the researchers are left with a numerical experiment. For the numerical integration of the three-body problem, it is necessary to set up the initial conditions: masses of the bodies, their coordinates and velocities. We need to choose for each body mass, 3 spatial coordinates and 3 initial velocities, 21 parameters in total. We can slightly reduce this number using the integrals of motion, but still the space of initial conditions will have a high dimension, which makes it difficult to choose the initial conditions and limits the ability to present the research results in a visual and easy-to-analyze form.

One can simplify the problem by considering all bodies of the same mass. Next simplification is to choose zero initial velocities. This simplifies the problem - from the spatial the problem becomes planar. In this case, it is necessary to specify initial coordinates of the bodies, 3 pairs, six numbers total, but the dimensionality is still high and does not allow visualization easily. The problem was solved when the famous region D appeared [1, 2], often called Agekian-Anosova region D or Agekian-Anosova map. Later, A.D. Chernin proposed the name homology region D [3].

The idea of the region D is very simple: if we place two bodies at the points with coordinates (-0.5, 0) and (0.5, 0), then we get all possible different geometric configurations by placing the third body in the area bounded by (positive) coordinate axes and arc of the unit circle centered at (-0.5, 0), see Fig. 1.

Introduction of the homology region D allows sistematical study of the free-fall equal mass three-body problem and natural visualization. One can study and display, e.g., life-time of the systems, see Fig. 2, or search for initial conditions leading to two- and three-body collisions after first, second, etc. approach (Fig. 3), analyse complecsity of trajectories (Fig. 4) and so on.

Homology region D can also be used as a map [4]: at any moment of time to analyze geometric configuration we can project the system into region D and

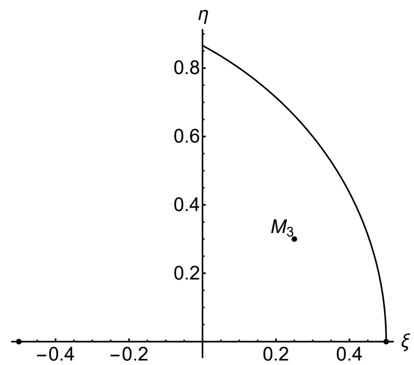


FIGURE 1. Agekian-Anosova Region D.

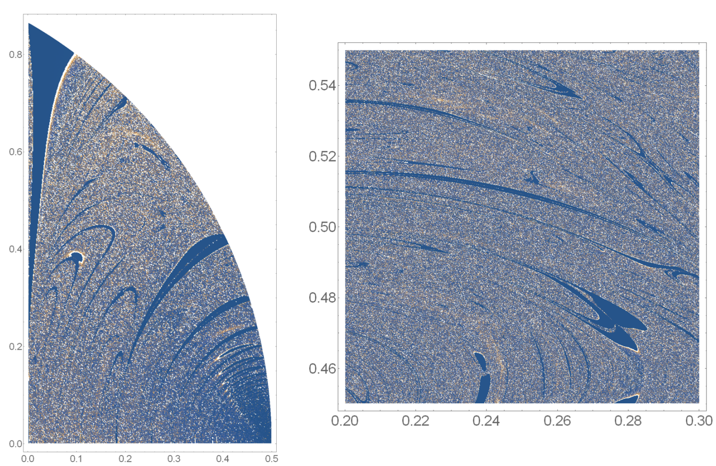


FIGURE 2. Left: Life time of three-body systems. Blue (dark) color correspond to short-living systems. Right: zoom into selected area.

follow the motion of the point representing the system. It can be done also in the case of non-planar (3D) motion. Since typical final stage of the evolution of three-body system with zero angular momentum is ejection, the point (0.5, 0) will play a role of attractor. Region D can be generalized to the case of different masses - in this case one would need to consider all six possible permutations of the bodies at the initial moment.

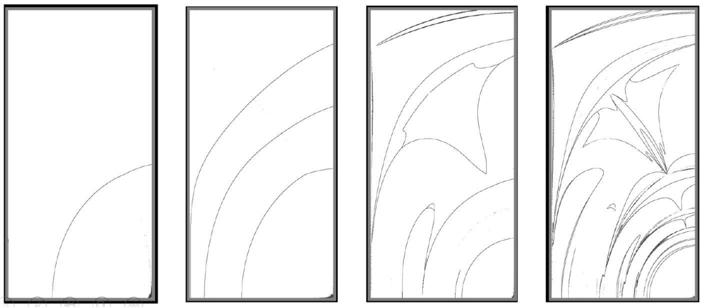


FIGURE 3. Two-body collision curves after first, second, etc. approach. Triple collisions can be revealed as intersections of the curves.

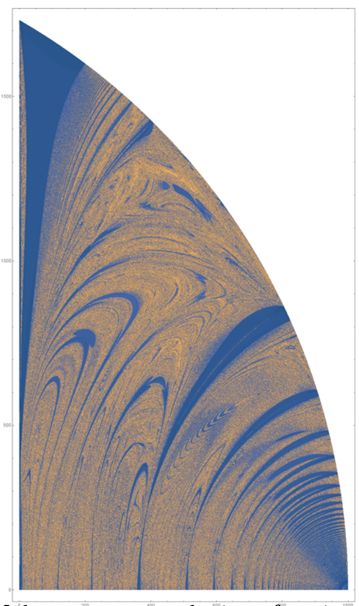


FIGURE 4. Kolmogorov complexity of trajectories. For each trajectory symbolic sequence was constructed. Complexity is estimated as a length of the archived sequence.

References

[1] Agekian T. A., Anosova J. P. *Astron. Zh.*, 44, 1261; Soviet Astron. 2, 1006, 1967

[2] Agekian T. A., Anosova J, P. *Astrofizika*, 4, p. 31, 1968

[3] Chernin A., Ivanov A., Mikkola S.) *Astron. and Astrophys.*, V. 281. p. 685, 1994

[4] Mauri Valtonen, Hannu Karttunen *The Three-Body Problem*, Cambridge University Press, 2009

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

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

Around concurrent normal conjecture

Alexandr Grebennikov and Gaiane Panina

Given a smooth convex body $K \in \mathbb{R}^n$, its normal to a point $p \in \partial K$ is a line passing through p and orthogonal to ∂K at the point p. It is conjectured that for any convex body $K \in \mathbb{R}^n$ there exists a point in the interior of K which is the intersection point of at least $2n$ normals from different points on the boundary of K. The concurrent normals conjecture trivially holds for $n = 2$. For $n = 3$ it was proven by Heil via geometrical methods and reproved by Pardon via topological methods. The case $n = 4$ was completed also by Pardon.

Recently Martinez-Maure proved for $n = 3, 4$ that (under mild conditions) almost every normal through a boundary point to a smooth convex body K passes arbitrarily close to the set of points lying on normals through at least six distinct points of ∂K. He used Minkowski differences of smooth convex bodies, that is, the *theory of hedgehogs*.

We give a very short proof of a slightly more general result: *for dimension $n \geq 3$, under mild conditions, almost every normal through a boundary point to a smooth convex body $K \in \mathbb{R}^n$ contains an intersection point of at least 6 normals from different points on the boundary of K.*

Our proof is based on the bifurcation theory and does not use hedgehogs.

Acknowledgments. G. Panina is supported by RFBR grant 20-01-00070A; A. Grebennikov is supported by Ministry of Science and Higher Education of the Russian Federation, agreement 075-15-2019-1619.

Alexandr Grebennikov
Department of Mathematics and Computer Sciences
Saint-Petersburg State University
Saint-Petersburg, Russia
e-mail: `sagresash@yandex.ru`

Gaiane Panina
Dept. name of organization
Saint-Petersburg Department of Steklov Mathematical Institute
Saint-Petersburg, Russia
e-mail: `gaiane-panina@rambler.ru`

Hidden symmetry of certain rational functions

Fedor Petrov

We discuss a non-obvious symmetry of a certain sum of rational weights along non-intersecting lattice paths. Based on a joint work with I. Pak. The talk is based on a current work in progress joint with I. Pak.

Fedor Petrov
Department of Mathematics and Computer Science
St. Petersburg State University
St. Petersburg, Russia
e-mail: `f.v.petrov@spbu.ru`

On some numerical experiments with character sums over finite fields

N. V. Proskurin

Abstract. By numerical experiments, it is discovered some strictures in distribution of cubic exponential sums in finite fields. It is given a conjecture on distribution of these sums.

Consider the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ of prime order p, its additive character

$$x \mapsto e_p(x) = \exp(2\pi i x/p), \quad x \in \mathbb{F}_p,$$

a one-variable polynomial f over $\mathbb{F}_p$ and related [1], [2] character (or exponential) sum of additive type

$$\sum_{x \in \mathbb{F}_p} e_p\bigl(f(x)\bigr). \tag{1}$$

By Weil, the fundamental inequality

$$\Bigl|\sum_{x \in \mathbb{F}_p} e_p\bigl(f(x)\bigr)\Bigr| \le (\deg f - 1)\sqrt{p}$$

is valid for all the sums whenever $p \nmid \deg f$. That means, the points

$$E_p(f) = \frac{1}{(\deg f - 1)\sqrt{p}} \sum_{x \in \mathbb{F}_p} e_p\bigl(f(x)\bigr) \tag{2}$$

are located in the unit disk $D = \bigl\{ z \in \mathbb{C} \bigm| |z| \le 1 \bigr\}$.

Let f be a one-variable polynomial over $\mathbb{Z}$. By reduction its coefficients $\bmod p$, we may consider f as a polynomial over any $\mathbb{F}_p$. Then one may look on distribution of the points $E_p(f)$ $(p = 2, 3, 5, 7 \ldots)$ in the disk D. One may also look on distribution of the points $|E_p(f)|$ $(p = 2, 3, 5, 7 \ldots)$ in the interval $[0, 1]$. We have studied numerically the sums (1) for lot of cubic polynomials f. We have used computer algebra systems PARI and MAPLE. Our main observations are as follows.

(I) For any positive $x \in \mathbb{R}$, let $\pi(x)$ be the number of prime $p \le x$. Given a cubic polynomial f, some positive $X \in \mathbb{R}$, and some interval $\Omega \subset [0,1]$ consider

$$\frac{1}{\pi(X)} \sharp \left\{ p \le X \;\middle|\; |E_p(f)| \in \Omega \right\}. \tag{3}$$

We may take $\Omega = [0,z]$ with $z \in [0,1]$ to treat (3) as a function of z. We find numerically (for many different f and large X) very good agreement of the function (3) with the function

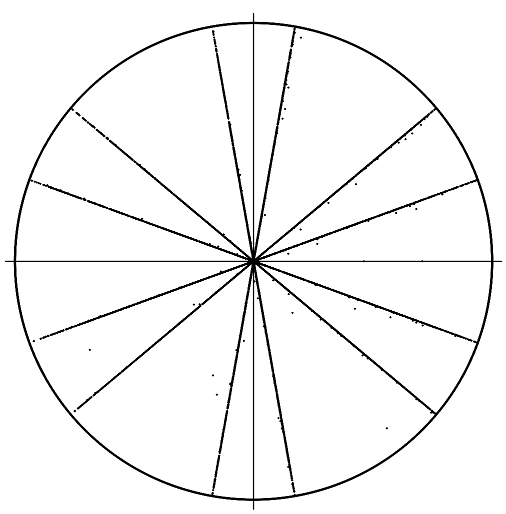
$$z \mapsto \frac{4}{\pi} \int_0^z \sqrt{1-x^2}\, dx.$$

Based on this observation, *we conjecture*

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sharp \left\{ p \le x \;\middle|\; |E_p(f)| \in \Omega \right\} = \frac{4}{\pi} \int_\Omega \sqrt{1-x^2}\, dx$$

for all cubic polynomials f *and all intervals* $\Omega \subset [0,1]$. That may be considered as an analogue of the classical Sato–Tate conjecture on distribution of the Kloosterman sums. The density on the right-hand side is known also in connection with the distribution of the numbers of points on elliptic curves.

(II) Let us consider one instructive sample. On the picture below we have plotted the real coordinate axis, the imaginary coordinate axis, the unit disk $D \subset \mathbb{C}$, and the points $E_p(f) \in D$ for the polynomial $f(x) = 6x^3 + 3x^2 + 4x$ and for all prime numbers $p \le 100000$.



The points $E_p(f)$ with $f(x) = 6x^3 + 3x^2 + 4x$ and prime $p \le 100000$.

It is seen that the points $E_p(f)$ are concentrated along 6 lines passing through the point 0. We see that the points $E_p(f)$ are just concentrated along the limit lines rather than lie on them. The counterclockwise angles between the lines and the real axis are $\pi m/3 + \pi n/9$ with $m = 0, 1, 2$ and $n = 1, 2$. The points distributed sporadically are those few $E_p(f)$ that are located far away from the limit lines.

We have found a similar aster-type pictures for many other cubic polynomials $ax^3 + bx^2 + cx + d$ over $\mathbb{Z}$. We have no theoretical explanation to this phenomenon. The number of lines depends on the coefficients a, b, c. Looking for possible classification, we may say the polynomial f falls to the class aster-m if we see m limit lines on the picture. In this sense, the above polynomial f falls to the class aster-6. Some other classes are given in [3].

References

[1] J.-P. Serre, *Majorations de sommes exponentielles*, Société Mathématique de France, Asterisque 41–42, p. 111–126, 1977.

[2] S. A. Stepanov, *Arithmetic of algebraic curves*, Moscow, 1991 (in Russian). English translation: Springer–Verlag, 1995.

[3] N. V. Proskurin, *On some cubic exponential sums*, Zap. Nauchn. semin. POMI, vol. 502, 122–132, 2021 (in Russian).

N. V. Proskurin
St. Petersburg Department of Steklov Institute of Mathematics RAS,
191023, Fontanka 27, St. Petersburg, Russia
e-mail: np@pdmi.ras.ru

Symbolic Inference for Non-Horn Knowledge Bases With Fuzzy Predicates

Alexander Sakharov

Abstract. This paper investigates non-Horn knowledge bases with fuzzy predicates. Inference from these knowledge bases excludes reasoning by contradiction, and it is characterized by means of substructural single-succedent sequent calculi with non-logical axioms expressing knowledge base rules and facts. A variety of truth functions can be used for the bodies of knowledge base rules and their contrapositives. Lower bounds of fuzzy truth values of ground literals are obtained by symbolically deriving the literals, building symbolic expressions from derivations trees, and evaluating these expressions.

In memory of Vladimir Gerdt

1. Introduction

The languages of logic programs and knowledge bases (KB) are usually based on first-order logic (FOL) [14]. In non-Horn KBs, facts are literals. Atoms are expressions $P(t_1, ..., t_k)$ where P is a predicate and $t_1, ..., t_k$ are terms. Literals are atoms or their negations. Non-Horn rules are expressions $A \Leftarrow A_1 \wedge ... \wedge A_k$, where $A, A_1, ..., A_k$ are literals. The advantages of non-Horn KB over Horn KBs and normal logic programs are discussed in [16].

KBs and logic programs may include computable (aka evaluable) functions and predicates [10]. They can be implemented as recursive functions in a functional programming language or as algorithms in a procedural programming language. The implementations of evaluable predicates serve to calculate the truth values of their atoms with constant arguments. Evaluable predicates do not have to be boolean, they may yield real numbers interpreted as fuzzy truth values. Recent advances in AI made it possible to implement some predicates as neural networks [4, 18, 17]. These networks yield the fuzzy truth values of atoms of neural predicates with constant arguments.

The principle of Reductio Ad Absurdum (RAA) states that if A is deduced from a hypothesis that is A's complement, then A is derivable. Reasoning by contradiction, i.e. with using RAA, is not quite adequate for KBs with evaluable predicates [15]. It will be explained later that reasoning by contradiction is not appropriate for KBs with fuzzy predicates either.

We introduce a set of very simple sequent calculi that characterize inference without reasoning by contradiction for non-Horn KBs. Resolution refutations [3] and other derivations steering clear of RAA are mapped to derivations in these calculi. This paper shows how to use symbolic inference methods for the calculation of lower bounds of the truth values of ground literals, i.e. literals without variables. Symbolic derivations of literals in the sequent calculi are the input of the calculation. This calculation is done by building ground symbolic expressions and evaluating them. It is executed in a linear time of the size of the derivations trees.

2. Non-Horn Knowledge Bases With Fuzzy Predicates

A substitution is a finite set of mappings of variables to terms. The result of applying a substitution to a formula or set of formulas is called its instance. We consider inference of ground literals, which are called goals, from non-Horn KBs containing evaluable functions and fuzzy predicates. Evaluable functions and predicates may be partial. Fuzzy truth values are usually real numbers from interval $[0, 1]$. For non-Horn KBs, it is more convenient to use interval $[-1, 1]$ for the representation of truth values. One represents true, minus one represents false. Other real numbers from interval $[-1, 1]$ represent fuzzy truth values.

Terms of evaluable functions with constant arguments are evaluated as soon as they appear in KB derivations. The same applies to atoms of neural and evaluable predicates with constant arguments. The evaluation may not terminate, in which case it is assumed that the truth value is zero. Any complete search strategy for inference from KBs with evaluable and neural predicates should continue and-or search [14] simultaneously with the evaluations including neural computations. If the evaluation of ground atom $A(...)$ yields a positive value above a certain threshold $h > 0$, then $A(...)$ is considered a fact. If the evaluation of this atom yields a negative value below $-h$, then $\neg A(...)$ is considered a fact.

All other predicates will be called derivable. As explained in [16], derivable predicates should be considered partial by default. In the presence of neural predicates, the truth values of ground atoms of derivable predicates should also be real numbers from interval $[-1, 1]$, that is, derivable predicates are fuzzy. We assume that KB facts could be fuzzy. It is expected that truth values lower than one and higher than h are assigned to fuzzy KB facts. One is the default truth value for the other KB facts.

Let $|A|$ denote the truth value of ground literal A. We rely on the traditional definition of the negation truth function for fuzzy KBs: $|\neg A| = -|A|$ [2]. The use of this truth function for negation is limited to the calculation of the truth values of negatibve literals. T-norms are usually considered in the literature as conjunction truth functions [7]. Other conjunction truth functions may be more appropriate for some KBs. We do not fix the conjunction truth function. The use of this function is limited to the calculation of the truth values of the bodies of KB rules.

Truth functions for disjunctions will not be used here, and the use of implication truth functions will be indirect. The meaning of KB rules is that the truth value of the rule body is a lower bound of the truth value of the head. Given that KB rules are implications and assuming that KB rules are not fuzzy, this semantics of KB rules is consistent with several implication truth functions for t-norms. For the Lukasiewicz, Godel, and product t-norms, $|A \Rightarrow B| = 1$ if $|A| \leq |B|$ [7].

It is explained in [16] why reasoning by contradiction is questionable for KBs containing partial functions or predicates. The same argument applies to KBs containing neural predicates. Consider two KB rules $P \Leftarrow Q$ and $P \Leftarrow \neg Q$. Here is reasoning by contradiction using these rules. Suppose P is false. The first rule implies that Q is false, and hence P is true by the second rule. Now suppose $|P| = 0$. If $|Q| = 0$ as well, then both rules are satisfied, but they do not provide any evidence that P is true or $|P| > 0$ at least.

3. Sequent Calculi

Let $-A$ denote the complement of A, i.e. it is the negation of atom A, and the atom of negative literal A. A sequent is $\Gamma \vdash \Pi$ where Γ is an antecedent and Π is a succedent [11]. Antecedents and succedents are multisets of formulas. KB inference and logic programming are concerned about the derivation of literals, i.e. sequents of the form $\vdash A$ where A is a literal. Consider single-succedent calculi in which formulas are literals. The only structural rule is *cut*.

$$\frac{\Gamma \vdash A \quad A, \Pi \vdash B}{\Gamma, \Pi \vdash B}\ cut$$

These sequent calculi do not have logical axioms. The following rule is the only logical rule. It replaces the standard negation rules and is applicable to axioms.

$$\frac{A, \Gamma \vdash B}{-B, \Gamma \vdash -A}\ swap$$

KB facts and rules can be treated as non-logical axioms [11]. Sequents of the form $\vdash A$ represent facts, and rules are represented by sequents of the form $A_1, ..., A_n \vdash A$ where $A, A_1, ..., A_n$ are literals. Variables can be replaced by any terms in instances of these axioms. The conclusions of *swap* applied to KB rules are known as contrapositives [19].

Definition 1. *L_{cs} is the set of sequent calculus instances in which formulas are literals, succedents contain one literal, the structural rule is cut, the logical rule is swap whose premises are axioms, and non-logical axioms represent KB rules and facts.*

Theorem 1. *L_{cs} is sound and complete with respect to the derivation of ground literals in FOL without RAA.*

Proof. It is proved in [15] that ground literal L is derivable from KB facts and rules in FOL without RAA if and only if $\neg L$ is refutable by resolution in which the factoring rule is not used and at least one premise of every resolution step is not $\neg L$ or its descendant. Consider such resolution refutation. The resolution steps that are not ascendants of the endclause are discarded. Let us ground this refutation and then exclude the step that resolves $\neg L$. There is only one such step because at least one premise of every resolution step is not $\neg L$ or its descendant. As a result, L is added to every descendant clause of this step including the endclause which becomes L.

Let us traverse this resolution tree bottom-up and map every resolution step to an application of *cut* in L_{cs}. Sequent $\vdash L$ is the conclusion of the last *cut* in the respective L_{cs} derivation tree. The premises of every *cut* in this tree are uniquely determined by the resolution step. The succedent of the *cut* conclusion is also the succedent of the second premise, and the succedent of the first premise is the principal formula of this *cut*. Every leaf node in the L_{cs} derivation tree is an instance of a KB fact, KB rule, or the conclusion of *swap* applied to an instance of a KB rule.

Now consider a ground L_{cs} derivation of sequent $\vdash L$. Every application of *cut* in this derivation corresponds to a resolution step but ground instances of KB rules and facts are used in this resolution derivation instead of the rules and facts. The endclause of this resolution derivation is L.

The lifting lemma [3] states that if clause A is an instance of A', B is an instance of B', and C is the resolvent of A and B, then there is such clause C' that C is its instance, and C' is the resolvent of A' and B'. It is well-known that the lifting lemma can be generalized onto arbitrary resolution derivations: If C is the endclause of a resolution derivation with input clauses $A_1, ..., A_n$ which are instances of $A'_1, ..., A'_n$, respectively, then there is such resolution derivation with input clauses $A'_1, ..., A'_n$ and endclause C' that C is an instance of C'. The proof is a straightforward induction on the depth of resolution derivations.

As a consequence of this generalization of the lifting lemma, there is a resolution tree with the input comprised of KB rules and facts treated as clauses and with such endclause L' that L is its instance. A step resolving L' and $\neg L$ is added to this derivation. The resolvent of this step is the empty clause, and $\neg L$ occurs in one premise of the last step only. □

4. Rule Truth Functions

Traditionally, the truth values for conjunction are defined in fuzzy KBs by the following equation: $|A_1 \wedge ... \wedge A_k| = \min\{|A_1|, ..., |A_k|\}$ [2]. With the Godel t-norm (min) as the truth function for KB rule bodies, a lower bound for the truth value of the head of rule $A_0 \Leftarrow A_1 \wedge ... \wedge A_k$ is given by inequality $|A_0| \geq \min\{|A_1|, ..., |A_k|\}$

according to the semantics of KB rules adopted here. Consider the case that $|A_i|$ are positive for $i = 1, ..., j-1, j+1, ..., k$, and $|A_0|$ is negative. As an implication of the semantics of KB rules, $|-A_j| \geq |-A_0|$ in this case. This inequality gives a lower bound for the truth values of the heads of KB rule contrapositives.

If we replace literal truth values with variables, then the right-hand side of the latter inequality can be viewed as the truth function for the body of contrapositive $-A_j \Leftarrow -A_0 \wedge A_1 \wedge ... \wedge A_{j-1} \wedge A_{j+1} \wedge ... \wedge A_k$, i.e. this truth function is defined as: $s'(x_0, x_1, ..., x_{j-1}, x_{j+1}, ..., x_k) = x_0$. For brevity, truth functions for the bodies of KB rules or their contrapositives will be called rule and contrapositive functions, respectively. It was possible to obtain the contrapositive function because the rule function is defined by such symbolic expression $s(x_1, ..., x_k)$ that inequality $x_0 \geq s(x_1, ..., x_k)$ is solved for x_j under the conditions: $x_1 > 0, ..., x_{j-1} > 0, x_{j+1} > 0, ..., x_k > 0, x_0 < 0$.

For KBs conatining fuzzy predicates, another truth function for the conjunctions that are KB rule bodies could give more accurate lower bounds of the truth values of the respective rule heads. Linear functions do not seem a good choice for rule truth functions because they may yield positive values even when one argument is zero. This reason applies to the Lukasiewicz t-norm too [7].

The product t-norm [7] does not look like a good choice either. The product t-norm is defined as the product of the truth values of literals in a conjunction provided that the truth values are in interval $[0, 1]$. For example, $0.6 * 0.6 = 0.36$. Linearly projecting these values into interval $[-1, 1]$, we would get the lower bound $|A_0| \geq -0.28$ for rule $A_0 \Leftarrow A_1 \wedge A_2$ and $|A_1| = |A_2| = 0.2$. The estimate 0.36 makes sense in a probabilistic setting, but the corresponding estimate for non-Horn KB rules is useless.

In contrast to the product t-norm, the following truth function for non-Horn KB rule bodies is more reasonable:

$s(x_1, ..., x_k) = \sqrt[k]{(x_1 + 1)...(x_k + 1)} - 1$

where k is the number of literals in the rule body. Given this rule function, a lower bound for the truth values of the heads of KB rule contrapositives could be obtained by solving the inequality $|A_0| \geq \sqrt[k]{(|A_1| + 1)...(|A_k| + 1)} - 1$ for $|-A_j|$:

$|-A_j| \geq 1 - (1 - |-A_0|)^k / ((|A_1| + 1)...(|A_{j-1}| + 1)(|A_{j+1}| + 1)...(|A_k| + 1))$

Again, replacing literal truth values with variables in the right-hand side of this inequality defines the contrapositive function associated with s.

Rule functions could be parametrized. For example, they could be parametrized by weights assigned to predicates. Also, custom functions yielding lower bounds for the truth values of rule heads could be defined for particular KB rules as it is done in Sugeno KBs [2]. Let $w(A)$ be the weight assigned to the predicate of literal A. Here is an example of a parametrized truth function:

$s(x_1, ..., x_k) = (x_1 + 1)^{w(A_1)/w} ... (x_k + 1)^{w(A_k)/w} - 1$

where s is defined for rule $A_0 \Leftarrow A_1 \wedge ... \wedge A_k$, and $w = w(A_1) + ... + w(A_k)$.

Definition 2. *Rule or contrapositive truth function s is called proper if $s(1,...,1) = 1$, $s(0,...,0) = 0$, and for $j = 1...k$, $h \leq s(x_1,...,x_j,...,x_k) \leq s(x_1,...,x'_j,...,x_k)$ if $x_j \leq x'_j$ and $x_1 \geq h,...,x_k \geq h$.*

It is easy to verify that the rule and contrapositive functions specified earlier satisfy the conditions of this definition.

5. Truth Value Approximation

Let $\alpha\{b_1 \to \beta_1,...,b_j \to \beta_m\}$ denote the substitution of term β_i for all occurrences of variable b_i in term α for $i = 1,...,m$. Let us define symbolic expression (term) $n(\tau)$ recursively for all ground derivations τ. In the following definition, lower-case letters are variables. These variables correspond to the same named upper-case ground literals.

- If τ is ground instance A of a KB fact, then $n(\tau) = |A|$ ($|A|$ is a constant).
- If τ is a ground instance $A_0 \Leftarrow A_1,...,A_k$ of KB rule and s is the truth function for this KB rule, then $n(\tau) = s(a_1,...,a_k)$.
- If the last rule of τ is *swap* with the conclusion $A_0, A_1,...,A_{j-1}, A_{j+1},...,A_k \vdash A_j$ and s' is the truth function for the respective contrapositive, then $n(\tau) = s'(a_0, a_1,...,a_{j-1}, a_{j+1},...,a_k)$.
- If the last rule of τ is *cut* with premises $A_1,...,A_k \vdash E$ and $E, C_1,...,C_m \vdash D$, then $n(\tau) = n(\nu)\{e \to n(\mu)\}$. Here, μ and ν are the parts of τ whose endsequents are the first and second premise of this *cut*, respectively.

Theorem 2. *If τ is a ground L_{cs} derivation of literal G and all rule and contrapositive functions are proper, then $|G| \geq n(\tau) \geq h$.*

Proof. By a straightforward induction of the depth of derivations, the only variables occurring in $n(\tau)$ are the variables corresponding to literals in the antecedent of the endsequent of τ. Consequently, $n(\tau)$ does not contain variables for any derivation τ with the endsequent $\vdash G$. All functions occurring in any $n(\tau)$ are increasing with respect to every argument. If $n(\tau)$ is treated as a function of the variables occurring in it, $n(\tau)$ is increasing with respect to every argument. It is proved by a straightworward induction on the depth of $n(\tau)$.

The value of any function from $n(\tau)$ is greater or equal to h if all arguments of this function are greater or equal to h. By induction on the depth of $n(\tau)$, the value of $n(\tau)$ is greater or equal to h if the value of every variable and every constant in it is greater or equal to h. Since the only constants in any $n(\tau)$ are the truth values of ground instances of KB facts, $n(\tau) \geq h$ for any τ whose endsequent is $\vdash G$.

Now we will prove by induction on the depth of derivations that if $A_1,...,A_k \vdash D$ is the endsequent of derivation μ, then $|D| \geq n(\mu)\{a_1 \to |A_1|,...,a_k \to |A_k|\}$. As a corollary, $|G| \geq n(\tau)$.

Base: The depth of derivation μ is zero. If the endsequent of μ is $\vdash D$, then D is an instance of a KB fact, and the above inequality holds. If the endsequent of μ is $A_1, ..., A_k \vdash D$, then this sequent is a KB rule instance, it does not contain constants, and the above inequality holds due to the definition of proper functions.

Induction step. Suppose the inequality under consideration is satisfied for all derivations whose depth is less or equal n. Suppose the depth of μ is $n+1$. If the last rule in μ is *swap*, then its premise is a ground instance of a KB rule, μ does not contain constants, and again, the inequality holds due to the definition of proper functions.

Now let the last rule in μ be *cut*, the first premise of this *cut* be $B_1, ..., B_k \vdash C_1$, and the second premise be $C_1, ..., C_m \vdash D$. If γ is the derivation ending in $B_1, ..., B_k \vdash C_1$ and δ is the derivation ending in $C_1, ..., C_m \vdash D$, then $|C_1| \geq n(\gamma)\{b_1 \rightarrow |B_1|, ..., b_k \rightarrow |B_k|\}$ and $|D| \geq n(\delta)\{c_1 \rightarrow |C_1|, ..., c_m \rightarrow |C_m|\}$ by the induction assumption. Due to the monotonicity of n with respect to every variable, $|D| \geq n(\delta)\{c_1 \rightarrow n(\gamma)\{b_1 \rightarrow |B_1|, ..., b_k \rightarrow |B_k|\}, ..., c_m \rightarrow |C_m|\}$. By the definition of n, $n(\mu) = n(\delta)\{c_1 \rightarrow n(\gamma)\}$. Hence, $n(\delta)\{c_1 \rightarrow n(\gamma)\{b_1 \rightarrow |B_1|, ..., b_k \rightarrow |B_k|\}, ..., c_m \rightarrow |C_m|\} = n(\mu)\{b_1 \rightarrow |B_1|, ..., b_k \rightarrow |B_k|, ..., c_m \rightarrow |C_m|\}$. □

This theorem establishes that $n(\tau)$ is a conservative approximation of the truth value of G. The proof of Theorem 1 shows that resolution refutations without factoring can be transformed to L_{cs} derivations in a single preorder traversal of the resolution derivations. Therefore, the time complexity of this transformation is linear in the size of the derivations. We focus on resolution methods because they are known to be more efficient.

It is clear from the proof of Theorem 2 that the calculation of a lower bound of $|G|$ can be done in a single postorder traversal of the derivation tree. We assume that the time complexity of algorithms implementing rule and contrapositive functions is linear in the number of function arguments. It is usually possible to implement such algorithms approximating these functions. Consequently, the calculation of a lower bound of $|G|$ takes a linear time of the size of G's derivation in L_{cs}.

Note that lower bounds of the truth values of derived ground literals could not be expressed via terms like n in the presence of RAA. RAA steps eliminate literal $-A$ from sequents $... -A... \vdash A$. The inequality from Theorem 2 for this sequent has the form $|A| \geq n(...)$ where $n(...)$ contains $|-A|$. This inequality does not give a lower bound for $|A|$.

It is feasible to get multiple derivations of the same goal. These derivations of one literal may give various approximations of the truth value of this literal. It may be beneficial to skip some fact instances with truth values close to h during the derivation process. The design of efficient inference methods capturing higher truth values is beyond the scope of this paper. Investigation of the applicability of non-proper truth functions is a topic for future research.

6. Related Work and Discussion

An overview of KB inference methods including resolution-based methods can be found in [14]. Resolution methods [3] are well suited for inference from non-Horn KBs. Ordered resolution is recognized as one of the most efficient inference methods [1]. It is used in modern theorem provers [8]. Ordered resolution has been adapted to inference from non-Horn KBs without RAA [15].

Like L_{cs}, LK_{-c} calculi from [16] contain non-logical axioms representing KB rules and facts. LK_{-c} calculi characterize inference of literals from non-Horn KBs without using RAA. Those calculi have the same inference power as L_{cs} but they employ standard negation rules as opposed to the swap rule, they allow multiple literals in succedents. LK_{-c} derivations cannot be directly used for the approximation of fuzzy truth values.

Our method is quite different from fuzzy KB systems [2], it does not involve fuzzification or defuzzification. Forward chaining normally serves as the inference mechanism for fuzzy KBs [2]. KB inference without RAA is more powerful than the forward application of Modus Ponens in chaining. For non-Horn KBs with neural and evaluable predicates, symbolic inference is done first. After that, a symbolic expression denoting a truth value is built from the derivation tree. Finally, this expression is evaluated.

Non-Horn KBs with fuzzy predicates are similar to possibilistic logic [5] in the sense that in both of them real numbers are associated with derived ground literals. A survey of fuzzy proof theories in which numbers indicating truthness are attached to FOL formulas is presented in [6]. The major difference of our approach is that literals are the only FOL formulas involved in the KB formalism considered here. Instead of applying fuzzy truth functions to FOL formulas [7], we propagate constraints on the truth values of literals.

The neural-symbolic method from [13] utilizes weighted real-valued functions for calculating lower and upper bounds of the truth values of FOL formulas. Inference is implemented as alternating upward and downward passes over the structure of the formulas. Truth value bounds are adjusted during these passes. Modus Ponens and Modus Tollens are used to update truth value bounds. In our work, sequents play the role of premises of Modus Ponens, and the swap rule can be viewed as a form of Modus Tollens.

ProbLog [12] extends Prolog by associating probabilities with facts. It is assumed that all ground instances of a non-ground fact are mutually independent and share the same probability. ProbLog engines calculate approximate probabilities for inference goals. Non-Horn KBs with neural and evaluable predicates are not probabilistic, they are based on fuzzy logic [7]. DeepProbLog [9] extends ProbLog by allowing neural networks to be associated with facts instead of probabilities. The probabilities of ground instances of a fact are calculated by the neural network associated with the respective predicate. In contrast, we interpret the output of neural networks as fuzzy truth values of ground facts.

References

[1] Leo Bachmair and Harald Ganzinger. Resolution theorem proving. In *Handbook of automated reasoning*, pages 19–99. Elsevier, 2001.

[2] Laécio Carvalho de Barros, Rodney Carlos Bassanezi, and Weldon Alexander Lodwick. *A first course in fuzzy logic, fuzzy dynamical systems, and biomathematics: theory and applications*. Springer, 2017.

[3] Chin-Liang Chang and Richard Char-Tung Lee. *Symbolic logic and mechanical theorem proving*. Academic press, 1973.

[4] Honghua Dong, Jiayuan Mao, Tian Lin, Chong Wang, Lihong Li, and Denny Zhou. Neural logic machines. In *International Conference on Learning Representations*, 2019.

[5] Didier Dubois and Henri Prade. Possibilistic logic-an overview. In *Computational logic*, pages 197–255, 2014.

[6] Siegfried Gottwald. *A treatise on many-valued logics*. Research Studies Press, 2001.

[7] Petr Hájek. *Metamathematics of fuzzy logic*. Springer Science & Business Media, 2013.

[8] Laura Kovács and Andrei Voronkov. First-order theorem proving and vampire. In *International Conference on Computer Aided Verification*, pages 1–35. Springer, 2013.

[9] Robin Manhaeve, Sebastijan Dumančić, Angelika Kimmig, Thomas Demeester, and Luc De Raedt. Neural probabilistic logic programming in deepproblog. *Artificial Intelligence*, 298:103504, 2021.

[10] William McCune. Otter 3.3 reference manual and guide. Technical report, Argonne National Lab., 2003.

[11] Sara Negri and Jan Von Plato. *Structural proof theory*. Cambridge University Press, 2001.

[12] Luc De Raedt and Angelika Kimmig. Probabilistic (logic) programming concepts. *Machine Learning*, 100(1):5–47, 2015.

[13] Ryan Riegel, Alexander Gray, Francois Luus, Naweed Khan, Ndivhuwo Makondo, Ismail Yunus Akhalwaya, Haifeng Qian, Ronald Fagin, Francisco Barahona, Udit Sharma, et al. Logical neural networks. *arXiv preprint arXiv:2006.13155*, 2020.

[14] Stuart Russell and Peter Norvig. *Artificial Intelligence: A Modern Approach*. Prentice Hall Press, 3rd edition, 2009.

[15] Alexander Sakharov. Inference methods for evaluable knowledge bases. In *Software Engineering Application in Informatics*, Lecture Notes in Networks and Systems, pages 499–510. Springer, 2021.

[16] Alexander Sakharov. A logical characterization of evaluable knowledge bases. In *14th International Conference on Agents and Artificial Intelligence*, pages 681–688, 2022.

[17] Adam Santoro, David Raposo, David G Barrett, Mateusz Malinowski, Razvan Pascanu, Peter Battaglia, and Timothy Lillicrap. A simple neural network module for relational reasoning. *Advances in neural information processing systems*, 30, 2017.

[18] Luciano Serafini and Artur S. d'Avila Garcez. Logic tensor networks: Deep learning and logical reasoning from data and knowledge. In *Neural-Symbolic Learning and Reasoning*. CEUR-WS.org, 2016.

[19] Mark E Stickel. A Prolog technology theorem prover: a new exposition and implementation in Prolog. *Theoretical Computer Science*, 104(1):109–128, 1992.

Alexander Sakharov
Synstretch
Framingham, Massachusetts, USA
e-mail: mail@sakharov.net

Generic-Case Complexity of the Multiple Subset Sum Problem

Alexandr Seliverstov

Abstract. We consider generic-case complexity of the multidimensional subset sum problem. Several heuristic algorithms have been known. So, in 1994, Nikolai Kuzyurin published such an algorithm. Nevertheless, the more methods are known, the more opportunities exist for solving certain problems. We propose a sub-exponential algorithm to verify that there is no binary solution to a general system of sufficiently many linear equations with integer coefficients. Roughly speaking, the algorithm checks whether there exists a low-degree algebraic hypersurface passing through each point with binary coordinates but not intersecting the given affine subspace.

Introduction

The subset sum problem is NP-complete. A commonly held view was that its worst-case complexity cannot be sub-exponential [1, 2]. Moreover, if we restrict our computations by so-called linear machines, then the problem is proved hard [3].

Generic-case complexity of a decision problem is sub-exponential when the set of hard inputs is negligible (or empty), but almost all inputs can be solved in sub-exponential time. Moreover, the negligible set containing hard inputs can be discerned explicitly. Such algorithms are also known as deterministic errorless heuristics. An example of fast generic-case algorithm is the condensation method for computing determinants [4]. For general matrices, the method is very nice. Nevertheless, if some intermediate matrix contains a zero entry, then the algorithm can fails.

By means of variable elimination, searching for a $\{0, 1\}$ solution to a system of m linearly independent linear equations in n variables is reduced to a parallel check whether a binary solution to a subsystem in $n-m$ variables can be extended to a $\{0, 1\}$ solution to the whole system of equations in n variables. Hence, the initial problem is polynomial-time solvable when the difference between the number of variables and the number of linearly independent equations is bounded by a function of the type $n - m = O(\log_2 n)$. In this work, we consider generic-case complexity when both m and difference $n - m$ are sufficiently large.

The Kuzyurin Algorithm

Let us denote by A a $m \times n$ matrix with nonnegative entries and by $\mathbf{b}$ a column. One can enumerate all $\{0, 1\}$ solutions to the system of inequalities $A\mathbf{x} \leq \mathbf{b}$ using dynamic programming. If $m > 9 \log_2 n$ and some assumptions about the distribution of the entry values hold, then the average number of $\{0, 1\}$ solutions is polynomially bounded. Therefore, all solutions can be found in average polynomial time [5]. The proof is based on the tail bounds of the binomial distribution. Next, one can verify whether a $\{0, 1\}$ solution to the system of equations $A\mathbf{x} = \mathbf{b}$ exists. The crucial limitation on the applicability of the Kuzyurin algorithm is the requirement of nonnegativity of the matrix entries. Of course, any system of linear equations can be reduced to another system with nonnegative coefficients, but the distribution is warped.

Low-density Problems

Let the density of an instance of the subset sum problem with positive integer coefficients a_k be defined by $\frac{n}{\log_2 \max_k a_k}$. A polynomial-time algorithm is known for solving almost all instances of sufficiently low density using a subroutine for finding the shortest nonzero vector in a lattice [6, 7]. The multiple low-density problems are considered too [8].

1. Our Main Algorithm

Within the context of the generic-case complexity, we consider machines having three halting states. So, the machine not only rejects or accepts an input, but it can also halt in the vague halting state. The latter means denial of response. But such a failure is possible only on a small fraction of inputs.

Theorem 1. *There exist both constant c and machine with the vague halting state such that for all positive integers $d \geq 2$, n, and $m < n$ satisfying the inequality $(n - m + d)(n - m + d - 1) \leq md(d - 1)$ and for every m-tuple of linear forms $\ell_j(x_0, \dots, x_{n-m})$, where $n - m < j \leq n$, the machine either rejects the input or halts in the vague halting state in $O(n^{cd})$ arithmetic operations. If the machine rejects the input, then there is no $\{0, 1\}$ solution to the system of all inhomogeneous equations of the type $x_j = \ell_j(1, x_1, \dots, x_{n-m})$. Moreover, for every applicable integers d, n, and m, there exists a nonzero polynomial of degree at most $n^2(n-m+1)^{2d-4}$ in coefficients of all the linear forms ℓ_j such that if the machine halts in the vague halting state, then the polynomial vanishes.*

Proof. The algorithm (Fig. 1) verifies whether there exists a solution to a system of linear equations in at most $n(n-m+1)^{d-2}$ unknowns λ_{tk} and λ_{tj}. The sufficient condition for the solvability is the full rank of a matrix. Of course, the rank can

FIGURE 1. Checking whether the system has no $\{0,1\}$ solution.

Input: Both integer $d \geq 2$ and set of m linear forms ℓ_j in $n-m+1$ variables.
if there exist numbers λ_{ik} and λ_{ij} such that

$$\sum_t \left(\sum_{k=1}^{n-m} \lambda_{tk} x_k (x_k - x_0) + \sum_{j=n-m+1}^{n} \lambda_{tj} \ell_j (\ell_j - x_0) \right) g_t = x_0^d,$$

where g_t is the t-th monomial of degree $d-2$ in variables $x_0, \ldots, x_{n-m}$
then the machine **rejects** the input
else the machine halts in the **vague** halting state.

be calculated easily. But a weaker sufficient condition is that a largest minor does not vanish. The minor is a polynomial in matrix entries. An entry is a polynomial of degree at most two in coefficients of linear forms ℓ_j. Thus, the minor is a polynomial of degree at most $n^2(n-m+1)^{2d-4}$. This polynomial does not vanish identically. □

Roughly speaking, the algorithm checks whether there exists a hypersurface passing through each $\{0,1\}$ point but not intersecting the given affine subspace. Therefore, for given d, if the algorithm rejects a subsystem, then it rejects the whole system too.

If $n - m = O(\sqrt{n})$, then one can use a constant degree d. Thus, generic-case complexity is polynomial, cf. [9].

Theorem 2. *There exist both constant c and machine with the vague halting state such that for all positive integers $n > m \geq 4\log_2^4 n$ and for every m-tuple of linear forms $\ell_j(x_0, \ldots, x_{n-m})$, where $n - m < j \leq n$, the machine either rejects the input or halts in the vague halting state in $O\left(2^{cn/\log n}\right)$ arithmetic operations. If the machine rejects the input, then there is no $\{0,1\}$ solution to the system of all inhomogeneous equations of the type $x_j = \ell_j(1, x_1, \ldots, x_{n-m})$. Moreover, for every applicable integers n and m, if all coefficients of forms ℓ_j picked independently and uniformly at random from a set of cardinality $(1/\varepsilon)4^{\lceil n/\log_2 n \rceil}$, then the machine halts in the vague halting state with probability at most ε.*

Proof. Let us use Theorem 1 with parameter $d = \lceil n/\log_2^2 n \rceil$. There exists a nonzero polynomial of degree at most $4^{\lceil n/\log_2 n \rceil}$ in coefficients of all the linear forms ℓ_j such that if the machine halts in the vague halting state, then the polynomial vanishes. In accordance with the Schwartz–Zippel lemma, the machine halts in the vague halting state with probability at most ε. □

Conclusion

If all coefficients are nonnegative integers from a large set and picked independently at random, then the Kuzyurin algorithm has the advantage with high probability [5]. But our algorithm works over all integers. Moreover, for nonnegative coefficients, it can also give a quick answer when the Kuzyurin algorithm requires a long running time.

References

[1] D. Grigoriev, *Complexity of Positivstellensatz proofs for the knapsack*, Computational Complexity **10** (2001), 139–154. `https://doi.org/10.1007/s00037-001-8192-0`

[2] S. Margulies, S. Onn, D.V. Pasechnik, *On the complexity of Hilbert refutations for partition*, Journal of Symbolic Computation **66** (2015), 70–83. `https://doi.org/10.1016/j.jsc.2013.06.005`

[3] K. Meer, *A note on a $P \neq NP$ result for a restricted class of real machines*, Journal of Complexity **8**:4 (1992), 451–453. `https://doi.org/10.1016/0885-064X(92)90007-X`

[4] C.L. Dodgson, *Condensation of determinants, being a new and brief method for computing their arithmetical values*, Proceedings of the Royal Society of London **15** (1866), 150–155.

[5] N.N. Kuzyurin, *An integer linear programming algorithm polynomial in the average case*. In: A.D. Korshunov (eds.) Discrete Analysis and Operations Research. Mathematics and Its Applications, vol. 355, pp. 143–152. Springer, Dordrecht, 1996. `https://doi.org/10.1007/978-94-009-1606-7_11`

[6] J.C. Lagarias, A.M. Odlyzko, *Solving low-density subset sum problems*, Journal of the Association for Computing Machinery **32**:1 (1985), 229–246. `https://doi.org/10.1145/2455.2461`

[7] M.J. Coster, A. Joux, B.A. LaMacchia, A.M. Odlyzko, C.P. Schnorr, J. Stern, *Improved low-density subset sum algorithms*, Computational Complexity **2**:2 (1992), 111–128. `https://doi.org/10.1007/BF01201999`

[8] Y. Pan, F. Zhang, *Solving low-density multiple subset sum problems with SVP oracle*, Journal of Systems Science and Complexity **29** (2016), 228–242. `https://doi.org/10.1007/s11424-015-3324-9`

[9] A.V. Seliverstov, *Binary solutions to large systems of linear equations* (in Russian), Prikladnaya Diskretnaya Matematika **52** (2021), 5–15. `https://doi.org/10.17223/20710410/52/1`

Alexandr Seliverstov
Institute for Information Transmission Problems of the Russian Academy of Sciences (Kharkevich Institute), Moscow, Russia
e-mail: `slvstv@iitp.ru`

Automorphisms of Types and Cryptography

Sergei Soloviev

- **Main point** of this reflection is that we may use morphisms (transformations) of types in cryptography if we want to encrypt structured objects (elements of a type) instead of mere "texts".

  Example. Consider the type

  $$P = (A \to A) \to ... \to (A \to A) \to (A \to A).$$

  The elements of the "premises" are functions $f_i : A \to A$, and the "conclusion" consists of $f : A \to A$ as well. So an element $F : P$ is, e.g., the composition operator, $Ff_1...f_n = f : A \to A$. In an encrypted form the order of f_i may be changed and the composition $Ff_{\sigma(1)}...f_{\sigma(n)}$ useless for an unauthorized user.
- **In Type Theory** one may introduce categorical structure taking types as objects and closed terms $t : A \to B$ as morphisms (up to usual equivalence relation based on normalization).

  Identity Id_A is represented by $\lambda x : A.x : A \to A$.

  As usual, $t : A \to B, t^{-1} : B \to A$ are mutually inverse isomorphisms if $t^{-1} \circ t \equiv id_A$ and $t \circ t^{-1} \equiv id_B$.

  E.g., $\lambda z : B_1 \to (B_2 \to C).\lambda x_2 : B_2.\lambda x_1 : B_1.(zx_1x_2)$ is an isomorphism from $B_1 \to (B_2 \to C)$ to $B_2 \to (B_1 \to C)$

  It works for different systems of Type Theory and λ-calculus.
- **An automorphism** is an isomorphism $t : A \to A$§ e.g., $\lambda z : B \to (B \to C).\lambda x_2 : B.\lambda x_1 : B.(zx_1x_2)$ (i.e., we take $B_1 = B_2$ above).

  For each type A the automorphisms $A \to A$ form the group of automorphisms $Aut(A)$.

  It may be seen as a subcategory of the groupoid of isomorphisms, i.e., the subcategory of the category of types and deductions - or terms - with the same objects and only isomorphisms as morphisms.

  If we fix a type, we may consider also the groupoid $Gr(A)$ of types isomorphic to A.
- **Relevant theorems.**

  Theorem (Dezani-Ciancaglini, [1]). $\beta\eta$-invertible terms in the untyped λ-calculus are exactly the finite hereditary permutations (f.h.p.).

On calls *erasure* elimination of all type information from λ-terms in typed λ-calculus.

Based on this theorem, it is possible to establish that the (well-typed) terms in many systems of typed λ-calculus are isomorphisms iff their erasures are f.h.p.

Theorem (Soloviev [5]). The groups $Aut(A)$ for simple types A are (up to isomorphism of groups) exactly the groups that may be obtained from symmetric groups by cartesian product and wreath product.

(By an old Jordan's theorem: they are exactly the groups of automorphisms of finite trees. Not C_3 for example.)

Theorem (Soloviev [5]). For every finite group G there exists a type A_G in second order typed λ-calculus (system F) such that the group $Aut(A_G)$ is isomorphic to G. *Idem* for Z. Luo's typed logical framework LF with dependent types.

- **Interest to cryptography.** Illustration: **ElGamal** cryptosystem (cf. [3, 4]).

  The protocol may use the iterations of a distinguished automorphism $g : A \to A$, where g^m is $g \circ ... \circ g$ (m times).

  Private Key: $m, m \in N$. **Public Key:** g and g^m.

  Encryption. To send a message $a : A$ (in our approach it is not a plain text, but an element of type A, and may have more complex structure) Bob computes g^r and g^{mr} for a random $r \in N$. The ciphertext is $(g^r, g^{mr}a)$.

  Decryption. Alice knows m, so if she receives the ciphertext $(g^r, g^{mr}a)$, she computes g^{mr} from g^r, then $(g^{mr})^{-1}$, and then computes a from $g^{mr}a$.

  Remark. We do not consider here the cryptosystems like **MOR** based on a more sophisticated group theory [4] but they, too, can be represented in type theory using the results of [5].

  By encoding a finite cyclic group of prime order as a group of automorphism of some type we can implement ElGamal (or any other cryptographic protocol based on finite groups) since the composition and inverse of type automorphisms (represented by finite hereditary permutations [2]) can be computed in linear time.

  However, finite cyclic groups are not the only possibility. Let us recall that the longest period in the symmetric group S_n is given by Landau function $\sim n^{\sqrt{n}}$. It corresponds to $Aut(a \to ... \to a \to p)$. This gives an idea of the length of the periods of automorphisms $f \in Aut(A)$. Maximal period of an element in the group $Aut(A)$ may be quite high.
- **This approach is not yet "ready to use".** One of the difficulties: for a type isomorphism/automorphism in *normal form* it is easy to compute the inverse. And this is not good for cryptography.
- **To be explored:** why then the terms used for encoding have to be in normal form? Normalization of a term may give "size explosion". And reduction sequence may be quite long (more that exponential). So it would be good if applying the Encryption and Decryption we might avoid normalization.
- **Example.** (Not directly related to isomorphisms.)

It is well known that natural numbers may be represented by so called *Church numerals*. In their typed version (for a type A) the number n is represented by $\lambda x : A \to A.\lambda y : A.(x(...(xy)...)$ (x is repeated n times). This is obviously related to "unary representation" of natural numbers. The term above is normal. One may define arithmetical operations and other arithmetical functions by application of other λ-terms to numerals. (In fact, using untyped lambda calculus and corresponding version of numerals, any partial recursive function may be represented.)

However, one may define also λ-terms representing binary notation. It is enough to apply (in appropriate order) two terms t_0 and t_1 representing multiplication by 2 and multiplication by 2 plus 1, to the term representing 0. Curious observation is that binary numbers are thus represented by terms that are not normal. If we normalize them we obtain exponentially longer presentation by standard Church numerals. However, to execute arithmetical operations we do not need to normalize these terms. The familiar algorithms for binary numbers may be adjusted.

- **Conclusion.** Principal idea - to use encoding that preserves functional correctness of programs. It may be done by type automorphisms represented by λ-terms. We had shown that standard cryprographic schemes (like ElGamal) may be adjusted to this case. Some other problems that have to be solved to make the scheme workable (e.g., the use of normal versus non-normal terms) were outlined.

References

[1] Dezani-Ciancaglini, M. (1976) Characterization of normal forms possessing inverse in the $\lambda - \beta - \eta$-calculus. *Theoretical Computer Science* **2** 323-337.

[2] Di Cosmo, R. (1995) *Isomorphisms of types: from lambda-calculus to information retrieval and language design.* Birkhauser.

[3] Hoffstein, J., Pipher, J. and Silverman, J.H. (2008) An introduction to mathematical cryptography. Springer, New York.

[4] Mahalanobis, A. (2015) The MOR cryptosystem and finite p-groups. *Contemp. Math.*, **633**, 81-95.

[5] Soloviev, S., Malakhovski, J. (2018) Automorphisms of Types and Their Applications. (Engl.) Zap. N. Semin. POMI, 468: 287-308.

[6] Soloviev, S. (2019) Automorphisms of Types in Certain Type Theories and Representation of Finite Groups. *Math. Structures in Computer Science*, 29(4): 511-551.

Sergei Soloviev
IRIT
Universtité Paul Sabatier Toulouse 3
Toulouse, France
e-mail: Sergei.Soloviev@irit.fr

The Chvátal–Sankoff problem: Understanding random string comparison through stochastic processes

Alexander Tiskin

Abstract. Given two equally long, uniformly random binary strings, the expected length of their longest common subsequence (LCS) is asymptotically proportional to the strings' length. Finding the proportionality coefficient γ, i.e. the limit of the normalised LCS length for two random binary strings of length $n \to \infty$, is a very natural problem, first posed by Chvátal and Sankoff in 1975, and as yet unresolved. This problem has relevance to diverse fields ranging from combinatorics and algorithm analysis to coding theory and computational biology. Using methods of statistical mechanics, as well as some existing results on the combinatorial structure of LCS combined with elementary probability theory, we link constant γ to the parameters of a certain stochastic particle process. These parameters are determined by a specific (large) system of polynomial equations, which implies that γ is an algebraic number. Using a computer program for exhaustive enumeration of configurations of the relevant stochastic process for a sufficient number of time steps, we solve our system numerically. Short of finding a closed-form solution for such a polynomial system, which appears to be unlikely, our approach essentially resolves the Chvátal–Sankoff problem, albeit in a somewhat unexpected way with a rather negative flavour.

Alexander Tiskin
Department of Mathematics and Computer Science
St. Petersburg State University
St. Petersburg, Russia

Fast RSK correspondence by doubling search

Alexander Tiskin

Abstract. The Robinson–Schensted-Knuth (RSK) correspondence is a fundamental concept in combinatorics and representation theory. It is defined as a certain bijection between permutations and pairs of Young tableaux of a given order. We consider the RSK correspondence as an algorithmic problem, along with the closely related k-chain problem. We give a simple, direct description of the symmetric RSK algorithm, which is implied by the k-chain algorithm of Felsner and Wernisch. We also show how the doubling search of Bentley and Yao can be used as a subroutine by the symmetric RSK algorithm, replacing the default binary search. Surprisingly, such a straightforward replacement improves the asymptotic worst-case running time for the RSK correspondence that has been best known since 1998. A similar improvement also holds for the average running time of RSK on uniformly random permutations.

Alexander Tiskin
Department of Mathematics and Computer Science
St. Petersburg State University
St. Petersburg, Russia

Zero-velocity surfaces in the general three-body problem

Vladimir Titov

The zero velocity surfaces in the form space of the planar three-body problem are considered. Reduction by translations and rotations reduces the dimension of configuration space to 3. If the energy is negative the zero velosity surface has three branches. When angular momentum J equals to zero the available space is located inside the surface except for the origin. As J grows a small surface appears and increases around the origin. Inside this small surface the motion is impossible. The available space is located between two surfaces. As for restricted three body problem there are five different topological types of zero velosity surface depending on the value of J.

Lemaitre regularization is used for the degenerate cases, rectilinear and isosceles motions. In these cases, the configuration space are two-dimensional. The suitable parametrization yields the simple equations of motion in the regularized form space. The zero velocity curve bounds the available space. The properties of rectilinear and isosceles orbits in the regularized form space, including those that lead to chaotic motion, are studied. The number of orbits are calculated by numerical integration. Among them are the Schubart orbits and Brouke orbits, as well as free fall orbits (in rectilinear and isosceles cases).

The figure-eight orbit is considered in the regularized by Lemaitre form space. In this space figure-eight orbit has four pre-images. Clearly these pre-images passes through six pre-images of Euler points. It is interesting, that one of pre-images is approximately unit circle.

Vladimir Titov
The faculty of Mathematics and Mechanics
Saint-Petersburg State University
Saint Petersburg, Russia
e-mail: tit@astro.spbu.ru

Hierarchy of classicality indicators of N-level systems

Arsen Khvedelidze and Astghik Torosyan

The representation of finite-dimensional quantum systems in a phase space [1] inevitably leads to the problem of negativity of probability distributions defined over the phase space [2]. It is commonly accepted that this negativity is an essential attribute of "quantumness" of a system and therefore can be used for evaluation of the quantitative characteristics of states [3]. Following this idea and basing on the algebraic method of construction of the Wigner functions of $N-$level quantum systems [4, 5], we introduce the global indicator of classicality $\mathcal{Q}_N$ [6, 7, 8] defined as a relative volume of a subspace $\mathfrak{P}_N^{(+)} \subset \mathfrak{P}_N$ of the state space $\mathfrak{P}_N$, where the Wigner quasiprobability distribution is positive. In the present report we analyse a refined hierarchy of measures of classicality corresponding to a natural *stratification of state space* $\mathfrak{P}_N$ *by the unitary orbit types.* The adjoint action of $SU(N)$ group on density matrices $\varrho \in \mathfrak{P}_N$,

$$g \cdot \varrho = g\varrho g^\dagger\,, \qquad g \in SU(N)\,, \tag{1}$$

induces the state space decomposition into the strata:

$$\mathfrak{P}_N = \bigcup_{\text{orbit types}} \mathfrak{P}_{[H_\alpha]}\,. \tag{2}$$

The components of decomposition (2) are determined by the *isotropy group* H_ϱ of a point $\varrho \in \mathfrak{P}_N$,

$$\mathfrak{P}_{[H_\alpha]} := \left\{\varrho \in\ \mathfrak{P}_N |\ H_\varrho \text{ is conjugate to } H_\alpha\right\}. \tag{3}$$

Having in mind the above stratification, it is natural to define *global indicator of classicality* $\mathcal{Q}_N[H_\alpha]$ *of states over a given stratum* as the ratio:

$$\mathcal{Q}_N[H_\alpha] = \frac{\mathrm{Vol}\left(\mathfrak{P}^{(+)}_{[H_\alpha]}\right)}{\mathrm{Vol}\left(\mathfrak{P}_{[H_\alpha]}\right)}\,, \tag{4}$$

where $\mathfrak{P}^{(+)}_{[H_\alpha]}$ is the subset of stratum $\mathfrak{P}_{[H_\alpha]}$ where the Wigner quasiprobability distribution is non-negative. In the definition (4) the volumes are evaluated with respect to the Riemannian metric on $\mathfrak{P}_{[H_\alpha]}$ induced by the stratification embedding. In order to exemplify the introduced indicator of classicality, we explicitly evaluate the rate of quantumness-classicality for low-dimensional systems, such as a qubit and a qutrit.

References

[1] M. Hillery, R.F. O'Connell, M.O. Scully and E.P. Wigner, *Distribution functions in physics: Fundamentals*, Physics Reports, **106**(3), 121-167, 1984.

[2] R.L. Hudson, *When is the Wigner quasi-probability density non-negative?*, Reports on Mathematical Physics, **6**(2), 249-252, 1974.

[3] A. Kenfack and K. Zyczkowski, *Negativity of the Wigner function as an indicator of non-classicality*, J. Opt. B: Quantum Semiclass. Opt. **6**, 396-404, 2004.

[4] V. Abgaryan and A. Khvedelidze, *On families of Wigner functions for N-level quantum systems*, *https://arxiv.org/pdf/1708.05981.pdf* (2018).

[5] V. Abgaryan, A. Khvedelidze and A. Torosyan, *On the moduli space of Wigner quasiprobability distributions for N-dimensional quantum systems*, J. Math. Sci. **240**, 617-633, 2019.

[6] V. Abgaryan, A. Khvedelidze and A. Torosyan, *The Global indicator of classicality of an arbitrary N-Level quantum system*, J. Math. Sci. **251**, 301-314, 2020.

[7] N. Abbasli, V. Abgaryan, M. Bures, A. Khvedelidze, I. Rogojin and A. Torosyan, *On measures of classicality/quantumness in quasiprobability Representations of finite-dimensional quantum systems*, Physics of Particles and Nuclei, **51**, 443-447, 2020.

[8] V. Abgaryan, A. Khvedelidze and I. Rogojin, *On overall measure of non-classicality of N-level quantum system and its universality in the large N limit*, Lecture Notes in Computer Science, **12563**, 244-255, 2021.

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
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`

On Groebner bases in semigroup rings of partially ordered semigroups.

Nikolay Vassiliev

The paper discusses the theory of Groebner bases for ideals in semigroup rings of partially ordered semigroups. The finiteness theorems in classical theory, for example, the finiteness of reduced Grobner bases or the finiteness of the universal Grobner basis, are based on Dickson's lemma for a set of monomials of a finite number of variables and its generalization to decreasing ordinal ideals in the set of monomials. We prove analogs of Dixon's lemma for desdending ordinal ideals of Dicksonian partially ordered sets and give an answer to the question of finiteness of the universal Groebner bases in semigroup rings of partially ordered Dicksonian sets.

This work is carried out as part of a project supported by an RNF grant 21-11-00152

Nikolay Vassiliev
St. Petersburg Department of Steklov Institute of Mathematics,on
Saint Petersburg Electrotechnical University "LETI"
St.Petersburg, Russia
e-mail: vasiliev@pdmi.ras.ru

Bounded elementary generation of Chevalley groups

Boris Kunyavskiĭ, Eugene Plotkin and Nikolai Vavilov

Abstract. We state several results on bounded elementary generation and bounded commutator width for Chevalley groups over Dedekind rings of arithmetic type in positive characteristic. In particular, Chevalley groups of rank ≥ 2 over polynomial rings $\mathbb{F}_q[t]$ and Chevalley groups of rank ≥ 1 over Laurent polynomial rings $\mathbb{F}_q[t, t^{-1}]$, where $\mathbb{F}_q$ is a finite field of q elements, are boundedly elementarily generated. In both cases we establish explicit bounds, and in the latter case they are quite sharp. Using these bounds we can also produce explicit bounds of the commutator width of these groups. We also mention some applications, possible generalisations and several related open problems, whose solution would require explicit computations. The complete text of the present talk is available in [14].

Introduction

In the present talk, we consider Chevalley groups $G = G(\Phi, R)$ and their elementary subgroups $E(\Phi, R)$ over various classes of rings, mostly over Dedekind rings of arithmetic type (we refer to [34] for notation and further references pertaining to Chevalley groups, and to [2] for the number theory background).

Primarily, we are interested in the classical problems of estimating the width of $E(\Phi, R)$ with respect to the two following generating sets.

• The elementary generators $x_\alpha(\xi)$, $\alpha \in \Phi$, $\xi \in R$. We say that a group G is **boundedly elementarily generated** if $E(\Phi, R)$ has finite width $w_E(G)$ with respect to elementary generators.

• Commutators $[x, y] = xyx^{-1}y^{-1}$, where $x, y \in G$. We say that G has **finite commutator width** if every element of $E(\Phi, R)$ is a product of $\leq w_C(G)$ commutators $[x, y]$, $x \in G(\Phi, R)$, $y \in E(\Phi, R)$.

Research of Boris Kunyavskii and Eugene Plotkin was supported by the ISF grants 1623/16 and 1994/20. Nikolai Vavilov thanks the "Basis" Foundation grant N. 20-7-1-27-1 "Higher symbols in algebraic K-theory". The actual polynomial computations behind the present work were partially performed/verified with the help of `Mathematica 11.3`.

For the case of Chevalley groups of rank ≥ 2, in which we are mostly interested, bounded generation in terms of elementary generators, and bounded generation in terms of commutators are essentially equivalent. Indeed, in this case the Chevalley commutator formula readily implies that every elementary generator can be presented as a product of a bounded number of commutators.

Conversely, a very deep result by Alexei Stepanov and others, see, in particular, [30], and in final form [28], implies that every commutator in $E(\Phi, R)$ is a product of not more than L elementary generators, with the bound $L = L(\Phi)$ depending on Φ alone. But of course the actual estimates of $w_E(G)$ and $w_C(G)$ can be very different.

Both problems have attracted considerable attention over the last 40 years or so. Very roughly, the situation is as follows.

• Bounded elementary generation always holds with obvious *small* bounds for 0-dimensional rings. This follows from the existence of such short factorisations as Bruhat decomposition, Gauß decomposition, unitriangular factorisation of length 4, and the like. On the other hand, bounded generation usually fails for rings of dimension ≥ 2. But for 1-dimensional rings it is problematic.

• Existence of arbitrary long division chains in Euclidean algorithm implies that $\mathrm{SL}(2, \mathbb{Z})$ and $\mathrm{SL}(2, \mathbb{F}_q[t])$ are not boundedly elementary generated [6]. But this could be attributed to the exceptional behaviours of rank 1 groups.

• What came as a shock, was when Wilberd van der Kallen [13] established that bounded elementary generation — and thus also finite commutator width — fail even for $\mathrm{SL}(3, \mathbb{C}[x])$, a group of Lie rank 2 over a Euclidean ring! Compare also [8], for a slightly simplified proof.

An emblematic example of 1-dimensional rings are Dedekind rings of arithmetic type $R = \mathcal{O}_S$, for which bounded elementary generation of $G(\Phi, R)$ is intrinsically related to the positive solution of the congruence subgroup problem in that group. This connection was first noted by Vladimir Platonov and Andrei Rapinchuk, see [20].

For the **number case** the situation is well understood, even for rank 1 groups. Without attempting to give a detailed survey, let us mention some high points of this development. Apart from the rings $R = \mathcal{O}_S$, $|S| = 1$, with finite multiplicative group, such finiteness results are even available for $\mathrm{SL}(2, R)$.

• For all Chevalley groups of rank ≥ 2, after the initial breakthrough by Douglas Carter and Gordon Keller, [3, 4], later explained and expanded by Oleg Tavgen [31], and many others, we now know bounded elementary generation with excellent bounds depending on the type of Φ and the class number of R alone.

This leaves us with the analysis of the group $\mathrm{SL}(2, R)$, for a Dedekind ring $R = \mathcal{O}_S$, with infinite multiplicative group.

• At about the same time, jointly with Paige, Carter and Keller gave a model theoretic proof [unpublished], [5], somewhat refashioned by Dave Morris [18]. But as all model theoretic proofs, this proof gives no bounds whatsoever.

• On the other hand, another important advance was made by Cooke and Weinberger [7], who got excellent bounds, modulo the Generalised Riemann Hypothesis. The explicit unconditional bounds obtained thereafter seemed to be grossly exaggerated [16].

• Some 10 years ago Maxim Vsemirnov and Sury [36] considered the key example of $\mathrm{SL}\Big(2, \mathbb{Z}\Big[\frac{1}{p}\Big]\Big)$, obtaining the bound $w_E(\mathrm{SL}(2,R)) = 5$ *unconditionally*.

• This was a key inroad to the first complete unconditional solution of the general case with a good bound, in the work of Alexander Morgan, Andrei Rapinchuk and Sury [17]. The bound they gave is ≤ 9, but for the case when S contains at least one real or non-Archimedean valuation was almost immediately improved [with the same ideas] to ≤ 8 by Jordan and Zaytman [12].

However, the **function case** turned out to be much more recalcitrant, and is up to now not fully solved, apart from some important but isolated results. On the one hand, an analogue of Riemann's Hypothesis was known in this case for quite some time. Also, the function case analogue of Dirichlet's theorem on primes in arithmetic progressions, the Kornblum—Artin theorem for $\mathbb{F}_q[t]$, is much precise than the Dirichlet theorem itself.

On the other hand, in the positive characteristic additional arithmetic difficulties occur, that have no obvious counterparts in characteristic 0. They reflect in particular in the structure of arithmetic subgroups in the function case. For instance, it is well known that the group $\mathrm{SL}(2, \mathbb{F}_q[t])$ is not even finitely generated, whereas the groups $\mathrm{SL}(2, \mathbb{F}_q[t, t^{-1}])$ and $\mathrm{SL}(3, \mathbb{F}_q[t])$ are finitely generated but not finitely presented.

• Until very recently the only published result was that by Clifford Queen [23]. Queen's main result implies that under some additional assumptions on R — which hold, for instance, for Laurent polynomial rings $\mathbb{F}_q[t, t^{-1}]$ with coefficients in a finite field — the elementary width of the group $\mathrm{SL}(2,R)$ is 5. As we shall see this implies, in particular, bounded elementary generation of all Chevalley groups $G(\Phi, R)$ with plausible bounds.

Queen's proof is mainly based on the same principles proposed by Cooke and Weinberger [7] in the number field case. Namely, it uses subtle analytic ingredients, such as a function field analogue of Artin's primitive root conjecture, in order to obtain short division chains. In contrast to the number field case where the validity of Artin's conjecture is only known conditionally on the Generalized Riemann Hypothesis (GRH), its function field analogue, developed by Bilharz in the 1930's, became an unconditional theorem after Weil's work. See the paper of Lenstra [15] for more details, and for a strengthening of Queen's theorem.

• The case of the groups over the usual polynomial ring $\mathbb{F}_q[t]$ long remained open. Only in 2018 has Bogdan Nica established the bounded elementary generation of $\mathrm{SL}(n, \mathbb{F}_q[t])$, $n \geq 3$. Part of the problem is that in characteristic $p > 0$ bounded elementary generation is not the same as bounded generation in terms of cyclic subgroups. For instance, the groups $\mathrm{SL}(n, \mathbb{F}_q[t])$ do not have bounded generation in this abstract sense, see [1].

• After the preliminary version of the present work has been finished, there appeared a preprint of Alexander Trost [32] where the statement of our Theorem A was established for the ring of integers R of an arbitrary global function field K, with a bound of the form $L(d, q) \cdot |\Phi|$, where the factor L depends on q and of the degree d of K. His method is similar to Morris' approach in [18].

Here we merely state our main results. There are many interesting aspects of the proof, especially in the case of the group $\mathrm{Sp}(4, \mathbb{F}_q[t])$ that requires tons of explicit calculations, related to stability theorems, reciprocity laws, Mennicke symbols, Chebyshev polynomials, etc. Obviously, in the talk we can only present an outline, all details can be found in our paper [14].

1. Bounded generation of $G(\Phi, \mathbb{F}_q[t])$

Here we establish similar results for all Chevalley groups over $\mathbb{F}_q[t]$, with explicit uniform bounds that only depend on type Φ. The first major new result of the present work treats the most difficult example, polynomial rings $\mathbb{F}_q[t]$ with coefficients in finite fields.

Theorem A. *Let $G(\Phi, R)$ be a simply connected Chevalley group of type Φ, $\mathrm{rk}(\Phi) \geq 2$ over $R = \mathbb{F}_q[t]$. Then the width of $G(\Phi, R)$ with respect to elementary generators is bounded.*

One of the main points of the present work is that, unlike the proofs based on model theory, here we get *efficient* realistic estimates for the number of factors. In some cases, like for reduction to smaller rank, our bounds are the best possible ones. For small ranks, there might be still some gap between the counter-examples and the estimates we obtain, but our upper bounds are fairly close to the theoretically best possible ones. And the lower bounds in such similar problems are usually quite difficult to obtain, anyway.

Roughly, the leading idea of our proof still follows Tavgen's general scheme, and is based on his rank reduction trick. It is very general and beautiful, and works in many other related situations. Tavgen himself used the fact that for systems of rank ≥ 2 every fundamental root falls into the subsystem of smaller rank obtained by dropping either the first or the last fundamental root. However, as was pointed out by the referee of [26], the argument applies without any modification in a much more general setting. Namely, it suffices to assume that the required decomposition holds for *some* subsystems $\Delta = \Delta_1, \ldots, \Delta_t$, whose union contains all fundamental roots of Φ. These subsystems do not have to be terminal.

Some bound in the bounded generation for all Chevalley groups can be easily derived from the case of rank two systems by a version of the usual Tavgen's trick [31], Theorem 1, described in [35] and [26]. Let us state it in a slightly more general form.

Theorem B. *Let Φ be a reduced irreducible root system of rank $l \geq 2$, and R be a commutative ring. Further, let $\Delta_1, \ldots, \Delta_t$ be some subsystems of Φ, whose union contains all fundamental roots of Φ. Suppose that for all $\Delta = \Delta_1, \ldots, \Delta_t$, the elementary Chevalley group $E(\Delta, R)$ admits a unitriangular factorisation*

$$E(\Delta, R) = U(\Delta, R)U^-(\Delta, R) \ldots U^{\pm}(\Delta, R)$$

of length L. Then the elementary Chevalley group $E(\Phi, R)$ itself admits unitriangular factorisation

$$E(\Phi, R) = U(\Phi, R)U^-(\Phi, R) \ldots U^{\pm}(\Phi, R)$$

of the same length L.

Thus, we are left with the analysis of rank 2 cases.

• For A_2 bounded generation of $SL(3, \mathbb{F}_q[t])$ is precisely the main result of Nica [Ni]. In fact, Nica establishes that

$$w_E(SL(3, \mathbb{F}_q[t])) \leq 41.$$

This bound 41 is obtained as follows. Over a Dedekind ring one needs 7 elementary operations to reduce a 3×3 matrix to a 2×2 matrix (one would need 8 for a general ring subject to $sr(R) \leq 2$). The elementary length of any matrix $g \in SL(2, R)$ inside $SL(3, R)$ is at most 34. Interestingly, the main arithmetic ingredient of his proof is the Kornblum—Artin functional version of Dirichlet's theorem on primes in arithmetic progressions.

An interesting aspect of Nica's work [19] is that he avoids the usual Mennicke type calculations [2], and carries the proof using the so-called "swindling lemma" instead. This allows him to obtain somewhat better bounds for the number of elementary generators.

• Luckily, we do not have to imitate Tavgen's proof [31], section 5, for the case of the Chevalley group of type G_2. Instead of a difficult direct calculation, we show that this case can be derived from the case of A_2 by the usual stability arguments. Stability of the embeddings $A_1 \subseteq A_2 \subseteq G_2$ under $asr(R) \leq 2$ was established by Michael Stein, see [27]. We had just to go over the proof to trace all elementary operations.

Over a Dedekind ring one needs 20 elementary operations to reduce any element of $E(G_2, R)$ to an element of $SL(2, R)$ in a long root embedding — one would need 24 for a general ring subject to $asr(R) \leq 2$, which gives us

$$w_E(G(G_2, \mathbb{F}_q[t])) \leq 54.$$

• A large part of the actual proof of theorem A is the analysis of the most difficult case of $Sp(4, \mathbb{F}_q[t])$, which is the Chevalley group of type C_2. The difficulty is that now we have to take two types of embeddings of $A_1 \leq C_2$, the long root embedding and the short root embedding.

Here, we again take the proof in Tavgen's paper [31], section 4, as a prototype. But there is a substantial difference, since now we have to verify many arithmetic lemmas that are well known in the number case, but for which we could not find any obvious reference in the function case. Apart from a strong version of Kornblum—Artin theorem, we had to carry through rather meticulous calculations depending on the explicit formula of the reciprocity law for power-residue symbols.

Now, we have to first reduce the long root embedding to such an embedding whose entry is a square, then (following Bass—Milnor—Serre and Tavgen) reduce it to a short root embedding, and, finally, perform (more difficult!) calculations to express a matrix from $\mathrm{SL}(2, R)$ in the short root embedding as a product of elementary unipotents in $\mathrm{Sp}(4, R)$. As a result, the bound we get is worse than for other rank 2 cases.

This eventually leaves us with the [exaggerated] bound

$$w_E(G(\mathrm{C}_2, \mathbb{F}_q[t])) \leq 79.$$

and we challenge the reader to improve it, along the lines of [19].

Quite amazingly, C_2 is the only difficult case! For groups of types B_l and C_l, $l \geq 3$, we have found *much* easier proofs, based on the fact that *either* a long root, *or* a short one can be embedded in a root system of type A_2, so that we can proceed directly from [19].

In particular, for groups of rank 3 one gets *better* bounds than for C_2, viz.

$$w_E(G(\mathrm{C}_3, \mathbb{F}_q[t])) \leq 72, \qquad w_E(G(\mathrm{B}_3, \mathbb{F}_q[t])) \leq 65.$$

Some bounds for the elementary bounded generation for all Chevalley groups can be easily derived from the above form of Tavgen rank reduction theorem. For instance, it can be derived from the existence of two types of embeddings of $\mathrm{A}_2 \leq \mathrm{F}_4$, the long root embedding and the short root embedding, that

$$w_E(G(\mathrm{F}_4, \mathbb{F}_q[t])) \leq 216,$$

but this bound seems not to be the best possible.

For $\mathrm{SL}(n, R)$ there is a realistic bound of the width in elementary generators, in terms of stability conditions, taking into account the elementary fact that for Dedekind rings $\mathrm{sr}(R) = 1.5$. The above proof of Theorem A gives us occasion to return to the stability arguments for all Chevalley groups, and obtain bounds which are substantially better than the ones that could be obtained via Tavgen's trick.

Alternatively, Theorem A can be restated in the following equivalent form. The difference is that in this case the computations of many authors, subsumed and expanded by Andrei Smolensky [25], allow to produce short explicit bounds.

Theorem C. *Let $G(\Phi, R)$ be a simply connected Chevalley group of type Φ,* $\mathrm{rk}(\Phi) \geq 2$ *over $R = \mathbb{F}_q[t]$. Then $G(\Phi, R)$ is of finite commutator width L, where*

- *$L \leq 5$ for $\Phi = A_l$, for $l \geq 2$, or $\Phi = F_4$,;*
- *$L \leq 6$ for $\Phi = B_l, C_l, D_l$, for $l \geq 3$ or $\Phi = E_7, E_8$, or, finally, $\Phi = C_2, G_2$ under the additional assumption that 1 is the sum of two units in R (which is automatically the case, provided $q \neq 2$);*
- *$L \leq 7$ for $\Phi = E_6$.*

We believe that the bound for E_6 could be also improved to $L \leq 6$, but we were strongly discouraged by the extent of explicit calculations needed to do that.

2. Bounded generation of $G(\Phi, \mathbb{F}_q[t, t^{-1}])$

In fact, ulterior applications to Kac—Moody groups that we have in mind do not need the full power of Theorems A and C. We only need a similar result for the equally classical but *much easier* example of *Laurent* polynomial rings $\mathbb{F}_q[t, t^{-1}]$ with coefficients in finite fields.

For Chevalley groups over such rings bounded generation can be derived from Theorem A. Yet, the bounds thus obtained will not be the best possible ones. However, the multiplicative group of the ring $R = \mathbb{F}_q[t, t^{-1}]$ is *infinite*. This means that bounded generation — with much better bounds! — follows already from the result by Clifford Queen [23]. Let us state the most surpising finiteness result in terms of unitriangular factors obtained along this route.

Theorem D. *Let $R = \mathcal{O}_S$ be the ring of S-integers of K, a function field of one variable over $\mathbb{F}_q$ with S containing at least two places. Assume that at least one of the following holds:*

- *either at least one of these places has degree one,*
- *or the class number of R, as a Dedekind domain, is prime to $q-1$.*

Then any simply connected Chevalley group $G = G(\Phi, R)$ admits the following decompositions

$$G = UU^-UUU^- = U^-UU^-UU^-.$$

The key case here are the groups $\mathrm{SL}(2, R)$, for which the result follows from Theorem 2 of [23]. It is stated there correctly, but the proof at the very last page contains a minor inaccuracy and would imply that G admits a unitriangular decomposition of length 4, which contradicts the main result of [35]. The reason is that at a certain stage of the calculation one obtains an invertible element $\epsilon \in R^*$, whereas [23] takes this element to be 1. Slightly rearranging the proof, one gets the correct (and best possible!) bound, that any element of $\mathrm{SL}(2, R)$ is a product of ≤ 5 elementary transvections. Theorem C now follows by Tavgen's rank reduction trick.

In particular, this theorem allows to dramatically reduce bounds for groups over $\mathbb{F}_q[t, t^{-1}]$, to

$$w_E(G(\mathrm{A}_2, \mathbb{F}_q[t, t^{-1}])) \leq 15, \qquad w_E(G(\mathrm{C}_2, \mathbb{F}_q[t, t^{-1}])) \leq 20,$$
$$w_E(G(\mathrm{G}_2, \mathbb{F}_q[t, t^{-1}])) \leq 30,$$

via unitriangular factorisations. Stability results that we mentioned before afford even better bounds, such as, for instance,

$$w_E(G(\mathrm{A}_2, \mathbb{F}_q[t, t^{-1}])) \leq 12, \qquad w_E(G(\mathrm{C}_2, \mathbb{F}_q[t, t^{-1}])) \leq 15,$$
$$w_E(G(\mathrm{G}_2, \mathbb{F}_q[t, t^{-1}])) \leq 25.$$

As above, using the technology of [25], we can derive from Theorem D estimates for the commutator width.

Theorem E. *Let R be as in Theorem D. Then the commutator width of the simply connected Chevalley group $G = G(\Phi, R)$ is $\leq L$, where*

- $L = 3$ *for* $\Phi = A_l$*, for* $l \geq 2$*, or* $\Phi = F_4$*,;*
- $L = 4$ *for* $\Phi = B_l, C_l, D_l$*, for* $l \geq 3$ *or* $\Phi = E_7, E_8$*, or, finally,* $\Phi = C_2, G_2$ *under the additional assumption that* 1 *is the sum of two units in* R (*which is automatically the case, provided* $q \neq 2$);
- $L = 5$ *for* $\Phi = E_6$*;*

This kind of sharp bounds were quite unexpected for us. In particular, Chevalley groups over such *arithmetic* rings have the same commutator width as Chevalley groups over rings of stable rank 1, see [25].

3. Applications and possible generalisations

Primarily, we have in mind the following two types of applications, that are described in [14].

- Estimates of the width of Kac—Moody groups defined over a finite field with respect to commutators and other natural generating sets.
- Model-theoretic applications. Bounded generation implies a lot of important logical properties of groups. In our case the groups $G(\Phi, \mathbb{F}_q[t])$ and $G(\Phi, \mathbb{F}_q[t, t^{-1}])$, $\mathrm{rk}(\Phi) > 1$ turn out to be first order rigid, quasi-finitely axiomatisable and logically homogeneous.

Here are some generalisations of the above theorems A—E that we plan to address in the next papers.

- For all ranks $\mathrm{rk}(\Phi) \geq 1$ remove the remaining restrictions on the ring R in Theorems D and E.
- For ranks $\mathrm{rk}(\Phi) \geq 2$ prove analogues of Theorems A and C for all Dedekind rings of arithmetic type. This should be possible, but might be difficult, since many of the requisite arithmetic facts are not as easily available, as in the number case.
- For classical groups, reduction to smaller ranks is well-known. We are in possession of similar reduction results, based on effectivisation of [27, 21, 22, 9]. These results give pretty sharp bounds also for exceptional cases. But calculations with columns of height 26, 27, 56 and 248 are quite a bit more involved, and spread over several dozen pages.

In the next paper we plan to produce all details for the stability reduction for the exceptional cases F_4, E_6, E_7, E_8 in the same spirit as we have done in [14] for G_2, B_l and C_l. The goal is obtain new explicit bounds for the elementary width in these cases, which are better than the known ones even in the number case.

- Another very challenging problem would be to perform scrupulous analysis of the proofs to reduce the number of elementary moves. We are pretty sure that our bounds are far from being optimal. Even without attempting to get sharp bounds, we believe that we could improve the bounds in the present paper, and other related results.

However, to get the *best possible* bounds one might need to perform extensive computer search/computer calculations. However, to get such optimal bounds would be *extremely* difficult, no such bounds are in sight even in the number case, even for such groups as $\mathrm{SL}(3,\mathbb{Z})$.

• Partial positive results, such as bounded expressions of elementary conjugates and commutators in terms of elementary generators — decomposition of unipotents, Stepanov's univeral localisation, and the like, [29, 30, 28]. It seems one should be able to obtain similar results also for other word maps.

• Let us mention yet another extremely pregnant generalisation, **bounded reduction**. In fact, even below the usual stability conditions and even in the absense of the bounded generation for $G(\Phi, R)$, it makes sense to speak of the number of elementary generators necessary to reduce an element g of $G(\Phi, R)$ to an element of $G(\Delta, R)$, for a subsystem $\Delta \subseteq \Phi$.

One such prominent example are polynomial rings $R[t_1, \dots, t_m]$, where bounded reduction holds starting with a rank depending on R alone, not on the number of indeterminates. For the case of $\mathrm{SL}(n, R[t_1, \dots, t_m])$ this is essentially an effectivisation of Suslin's solution of the K_1-analogue of Serre's problem, explicit bounds were obtained in the remarkable paper by Leonid Vaserstein [33], which unfortunately remained unpublished. For other split classical groups such bounds were recently obtained by Pavel Gvozdevsky [10].

• Most of the results so far pertain to the *absolute* case alone. However, it makes sense to ask similar questions for the *relative* case, in other words for the congruence subgroups $G(\Phi, R, I)$, and the elementary subgroups $E(\Phi, R, I)$ of level $I \trianglelefteq R$. The expectation is to get similar *uniform* bounds in terms of the elementary conjugates $x_{-\alpha}(\eta)x_\alpha(\xi)x_{-\alpha}(-\eta)$, $\alpha \in \Phi$, $\xi \in I$, $\eta \in R$. Some results in this direction are contained in the paper by Sinchuk and Smolensky [24]. As a more remote goal one could think of generalisations to birelative subgroups, see [11].

We intend to return to [some of] these subjects in the full version of the present paper, and in its [expected] sequel.

Acknowledgements. Very special thanks go to Inna Capdeboscq. This work started jointly with her as a discussion of the bounded commutator width of various classes of Kac—Moody groups over finite fields, and for a long time [14] was supposed to result as a paper by *four* authors.

Our sincere thanks go to Olga Kharlampovich, Jun Morita, Alexei Myasnikov, Denis Osipov, and Igor Zhukov for useful discussions regarding various aspects of this work.

References

[1] M. Abért, A. Lubotzky, L. Pyber, *Bounded generation and linear groups*. Int. J. Algebra Comput. **13** (2003), 401–413.

[2] H. Bass, J. Milnor, J-P. Serre, *Solution of the congruence subgroup problem for* $\mathrm{SL}_n(n \geq 3)$ *and* $\mathrm{Sp}_{2n}(n \geq 2)$. Inst. Hautes Études Sci. Publ. Math. **33** (1967), 59–137.

[3] D. Carter, G. E. Keller, *Bounded elementary generation of* $\mathrm{SL}_n(\mathcal{O})$. Amer. J. Math. **105** (1983), 673–687.

[4] D. Carter, G. E. Keller, *Elementary expressions for unimodular matrices.* — Commun. Algebra **12** (1984), 379–389.

[5] D. Carter, G. E. Keller, E. Paige, *Bounded expressions in* $\mathrm{SL}(2,\mathcal{O})$, preprint Univ. Virginia, 1985, 1–21.

[6] P. M. Cohn, *On the structure of the* GL_2 *of a ring*. Inst. Hautes Études Sci. Publ. Math. **30** (1966), 5–53.

[7] G. Cooke, P. J. Weinberger, *On the construction of division chains in algebraic number rings, with applications to* SL_2. Commun. Algebra **3** (1975), 481–524.

[8] I. V. Erovenko, $\mathrm{SL}_n(F[x])$ *is not boundedly generated by elementary matrices: explicit proof*. Electronic J. Linear Algebra **11** (2004), 162–167.

[9] P. B. Gvozdevsky, *Improved* K_1*-stability for the embedding* D_5 *into* E_6. Commun. Algebra **48** (2020), 4922–4931.

[10] P. Gvozdevsky, *Bounded reduction of orthogonal matrices over polynomial rings*, `arXiv:2106.12697v1 [math.GR] 23 Jun 2021`, 19p.

[11] R. Hazrat, A. Stepanov, N. Vavilov, Z. Zhang, *Commutator width in Chevalley groups*. Note Mat. **33** (2013), 139–170.

[12] B. W. Jordan, Y. Zaytman, *On the bounded generation of arithmetic* SL_2. Proc. Nat. Acad. Sci. USA **116** (2019), 18880–18882.

[13] W. van der Kallen, $\mathrm{SL}_3(\mathbb{C}[X])$ *does not have bounded word length.* In 'Algebraic K-theory, Part I (Oberwolfach 1980)', 357–361, Lecture Notes in Math. **966**, Springer, 1982.

[14] B. Kunyavskiĭ, E. Plotkin, N. Vavilov *Bounded generation and commutator width of Chevalley groups: function case*, `arXiv:2204.10951v1 [math.GR], 22 Apr 2022`, 54p.

[15] H. W. Lenstra, *On Artin's conjecture and Euclid's algorithm in global fields.* Invent. Math. **42** (1977), 201–224.

[16] B. Liehl, *Beschränkte Wortlänge in* SL_2. Math. Z. **186** (1984), 509–524.

[17] A. V. Morgan, A. S. Rapinchuk, B. Sury, *Bounded generation of* SL_2 *over rings of* S*-integers with infinitely many units.* Algebra Number Theory **12** (2018), 1949–1974.

[18] D. Morris, *Bounded generation of* $\mathrm{SL}(n, A)$ (*after D. Carter, G. Keller, and E. Paige*). New York J. Math. **13** (2007), 383–421.

[19] B. Nica, *On bounded elementary generation for* SL_n *over polynomial rings.* Israel J. Math. **225** (2018), 403–410.

[20] V. P. Platonov, A. S. Rapinchuk, *Abstract properties of* S*-arithmetic groups and the congruence problem.* Izv. Ross. Akad. Nauk Ser. Mat. **56** (1992), no. 3, 483–508; English transl. in Russian Acad. Sci. Izv. Math. **40** (1993), 455–476.

[21] E. B. Plotkin, *Surjective stabilization for K_1-functor for some exceptional Chevalley groups.* Zapiski Nauch. Sem. LOMI **198** (1991), 65–88; J. Soviet Math. **64** (1993), 751–767.

[22] E. Plotkin, *On the stability of the* K_1*-functor for Chevalley groups of type* E_7. J. Algebra **210** (1998), 67–85.

[23] C. Queen, *Some arithmetic properties of subrings of function fields over finite fields.* Arch. Math. **36** (1975), 51–56.

[24] S. Sinchuk, A. Smolensky, *Decompositions of congruence subgroups of Chevalley groups.* Intern. J. Algebra Comput. **28** (2018), 935–958.

[25] A. Smolensky, *Commutator width of Chevalley groups over rings of stable rank* 1, J. Group Theory **22** (2019), 83–101.

[26] A. Smolensky, B. Sury, N. Vavilov, *Gauss decomposition for Chevalley groups, revisited.* Intern. J. Group Theory **1** 2011, 3–16.

[27] M. R. Stein, *Stability theorems for* K_1, K_2 *and related functors modeled on Chevalley groups.* Japan J. Math. (N.S.) **4** (1978), 77–108.

[28] A. Stepanov, *Structure of Chevalley groups over rings via universal localization.* J. Algebra **450** (2016), 522–548.

[29] A. Stepanov, N. Vavilov, *Decomposition of transvections: a theme with variations.* K-Theory **19** (2000), 109–153.

[30] A. Stepanov, N. Vavilov, *On the length of commutators in Chevalley groups*. Israel J. Math. **185** (2011), 253–276.

[31] O. Tavgen, *Bounded generation of Chevalley groups over rings of algebraic S-integers.* Izv. Akad. Nauk SSSR Ser. Mat. **54** (1990), no. 1, 97-–122; English transl. in Math. USSR Izv. **36** (1991), 101–128.

[32] A. A. Trost, *Bounded generation by root elements for Chevalley groups defined over rings of integers of function fields with an application in strong boundedness.* `arXiv:2108.12254v1 [math.GR], 27 Aug 2021`, 27p.

[33] L. N. Vaserstein, *Bounded reduction of invertible matrices over polynomial rings by addition operations.* Preprint Penn. State Univ., 2006, http://www.personal.psu.edu/lxv1/pm2.pdf.

[34] N. Vavilov, E. Plotkin, *Chevalley groups over commutative rings.* I: *Elementary calculations.* Acta Appl. Math. **45** (1996), 73–113.

[35] N. A. Vavilov, A. V. Smolensky, B. Sury, *Unitriangular factorizations of Chevalley groups.* Zap. Nauchn. Semin. POMI **388** (2011), 17–47; English transl. in J. Math. Sci., New York **183** (2012),584–599.

[36] M. Vsemirnov, *Short unitriangular factorizations of* $\mathrm{SL}_2(\mathbb{Z}[1/p])$. Q. J. Math. **65** (2014), 279–290.

Boris Kunyavskiĭ
Dept. of Mathematics
Bar-Ilan University,
Ramat Gan, Israel
e-mail: `kunyav@macs.biu.ac.il`

Eugene Plotkin
Dept. of Mathematics
Bar-Ilan University,
Ramat Gan, Israel
e-mail: plotkin@macs.biu.ac.il

Nikolai Vavilov
Dept. of Mathematics and Computer Science
St Petersburg State University
St Petersburg, Russia
e-mail: nikolai-vavilov@yandex.ru

Mathematics for Non-Mathematicians: an Idea and the Project

Vladimir Khalin, Nikolai Vavilov and Alexander Yurkov

Abstract. Mathematical education, both mass education, and university education of non-mathematicians, are in an abominable state, and rapidly degrading. We argue that the instruction of non-mathematicians should be dramatically reformed both as substance and style. With traditional approach, such a transformation would take decades, with unclear results. But we do not have this time. The advent of Computer Algebra Systems gives the mathematics community a chance to reverse the trend. We should make a serious attempt to seize this opportunity.

In the present talk we present *two* closely related such projects implemented at the St Petersburg State University:

• Developing education materials for teaching mathematics with the help of the *existing* Computer Algebra Systems, primarily `Mathematica` and `Maple`, as reflected in our book[32].

• Creating a *new* open source general purpose Computer Algebra System, with multilingual front-end, that could be used in teaching mathematics at the high school and university levels.

Introduction

We believe that the current situation with mathematical education, and the growing abyss between mathematicians and layman, even the educated ones, constitute an immediate desperate danger for our profession, and, eventually, for the whole human civilisation.

Over years, our efforts to incorporate computer algebra into mathematical education were supported by various bodies and institutions, including the St Petersburg State University, the Russian Ministry of Science and Higher Education, the Russian Foundation for Fundamental research (FRBR), and the Government of St Petersburg. The finalisation of the textbook [32] was sponsored by Vladimir Potanin's Foundation, grant GK180000694. At present, our work is supported by an educational project of the RFBR N. 19-29-14141.

The problem has been aggravated by the advent of computers, which can address vast majority of the traditional tasks, where Mathematics is applied, and whose mathematical software has no user serviceable parts. This has created a wide-spread illusion that now for the end-users there is no need to study any Mathematics whatsoever.

Our own assessment of the situation is EXACTLY THE OPPOSITE. To successfully function within their subject fields most professionals would now need to grasp much more Mathematics, and at that much deeper and more advanced Mathematics. Teaching non-mathematicians the necessary Mathematics in the same style we did before is simply not feasible.

We believe though, that, being part of the problem, computers can be also a decisive part of its solution. We describe a current project "MATHEMATICS AND COMPUTERS" implemented at the St Petersburg State University for the last 15 years. The concept is to focus exclusively on understanding and big ideas, while replacing most of the proofs and actual computational skills — apart from the most basic and the most enlightening ones — by computer calculations, experiments, and visualisation. The hard part was, of course, to develop a set of a few hundred test problems that would require *both* mathematical and algorithmic thinking. A fraction of our experience in this direction is reflected in the recent textbook [32].

Although we mostly discuss our teaching experience in St Petersburg, the problem itself seems to be of a very general nature, apparent in all technologically developed societies for several decades now. Compare, for instance, the 1981 lecture by Vladimir Rokhlin [27] or the 1990 article by William Thurston [29], which starts with the constatation: MATHEMATICS EDUCATION IS IN AN UNACCEPTABLE STATE. The interest of non-mathematicians in taking mathematics courses was constantly fading even then, see [16, 12]. However, it seems to us that the situation has *dramatically* exacerbated over the last 10–15 years, after computers have turned the tables.

1. Mathematics in human culture

Let us start with some self-evident truths:

- Spiritually and noetically, mathematics is, together with other higher creative arts, such as music or visual arts, the *paramount* manifestation of human culture.
- On the other hand, pragmatically we live in the world created by mathematics and science, in the first place by the *mathematische Naturwissenschaft*.
- Overall, it would not be a great exaggeration to assert, as Oswald Spengler did, that the level of a civilisation is largely determined by the level of its mathematics.

Unfortunately, these simple facts are rarely — if at all! — fully recognised not only by the general public, such as taxpayers, entrepreneurs, and polititians, but even by philosophers, journalists, educationalists and other discoursemongers.

In fact, most of the things around us, inlcuding ourselves, could not have existed in the present form without science. It starts simply with the sheer numerical strength of the human race (and other synanthropic animal species, such as cattle, pig, or sheep), which BY SEVERAL ORDERS OF MAGNITUDE exceeds the population of any other animal species of comparable body mass, and which would had been IMPOSSIBLE TO MAINTAIN WITHOUT SCIENCE.

Similarly, it is IMPOSSIBLE TO MAINTAIN — let alone to develop! — many of the PRESENT-DAY TECHNOLOGIES without a large number of individuals deeply congnisant in mathematics and science.

At various periods of history, Mathematics has been *extremely* successful in fostering the development of natural sciences, initially Astronomy and Physics, later on also other sciences and engineering.

We strongly believe that nowadays Mathematics *could* play a similar role in the development of life sciences, such as Biology and Medicine, as also in Linguistics, Psychology, Economics, etc.

Today, we even have most of the requisite tools and computational resources. What is lacking, however, is the **awareness** on the part of those who have to apply Mathematics in the respective subject fields. They do not know any Mathematics, they do not understand it, and they do not even understand why it is relevant — that Mathematics is the only feasible mediator between spirit and reality.

2. Mathematical education

The above explains an absolutely exceptional role played by mathematical education in the functioning of a society. As Jean Pierre Kahane stated it: IN NO OTHER SCIENCE HAS TEACHING AND LEARNING SUCH SOCIAL IMPORTANCE (cited in [4]).

Here, one should clearly distinguish

- Pre-university level — spectators;
- Mathematics for non-mathematicians — gentlemen;
- Mathematics for mathematicians — players.

Of these three, training professional mathematicians is the least problematic. We fully agree with Rokhlin that TEACHING MATHEMATICS TO THE WOULD-BE MATHEMATICIANS IS INFINITELY EASIER THAN TEACHING MATHEMATICS TO NON-MATHEMATICIANS, see [27]. If you know, understand and love your subject, and if you are honest with your students, it does not matter, whether you are an accomplished teacher, and what you do exactly, and how you do it. If they are *already* interested in Mathematics, you can relax, since you are bound to get through, regardless.

However, when working with the general public, or with other professionals, you should be at all time aware that you are working at three completely different levels:

- Mathematics as part of general culture;
- Mathematics *per se*;

- Mathematics for specific applications.

The fundamental flaw of the traditional mathematical education is that it is focusing on, and advertising the third aspect alone, which is invariably the least important one of all, mostly the least interesting one of all, and usually fictitious.

In our view, the single most important aspect of teaching mathematics at the elementary level is the cultivation of **intellectual honesty.** In other words, the ability to distinguish what you understand from what you don't, what was defined and has a precise meaning from what doesn't, what is said from what is intended, plausible from improbable, true from false, proven from conjectured, etc.

Another equally important aspect is the **callisthenics of mind**, as preparation to solve any kind of **difficult problems**. From this prospective, mathematics is a workout[1] that allows to develop, train and maintain inner vision, aesthetic taste, memory, tenue, concentration, the abilities to observe, compare, generalise and specialise, draw conclusions, follow and construct chains of arguments, etc.

What becomes progressively more important at further stages, especially when you train professionals in other fields, is the mathematical **mode of thinking** itself. The ability to start with the first principles, to take the simplest possible case and build up from there, to express things in a different language, to use analogies, to argue symbolically, to compress huge bulks of arguments, etc.

If we are trying to sell specific applications, we lose! That's exactly what is happening now, with devastating effects.

3. Utilitarian prospective

It is our deep conviction that UTILITARIAN PRINCIPLE DESTROYS EDUCATION. The best possible education is the useless one. The same applies to the mathematics education, of course.

In Europe the controversy between the supporters of a comprehensive approach to education, and the proponents of the practically-oriented one never subsided for the last 5 centuries, it seems. It suffices to recall the discord over the study of Latin and Greek in schools. Of course, this is indeed a huge social and economical issue, as we allude below.

But the debate itself is terribly much older than that. The polemic between Mo Di and Chuang-tze is still as relevant today, after 24 centuries, as it was in their life-time. But we are on the side of Chuang-tze, anyway: EVERYBODY KNOWS THE USEFULLNESS OF USEFUL THINGS. NOBODY KNOWS THE USEFULLNESS OF USELESS THINGS.

As we all know, Mathematics is an art form working with *ideas*, see [18], and, as Oscar Wilde observed, ALL ART IS QUITE USELESS. It is amazing, how often the word "useful" is repeated in Hardy's "Apology", dozens of times. Here is the most famous such instance, and the one most applicable to education:

[1] When asked "What kind of exercise do you prefer?", our colleague Timothy O'Meara responded: "Well, I'M EXERCISING MY BRAIN".

> One rather curious conclusion emerges, that pure mathematics is on the whole DISTINCTLY more useful than applied. A pure mathematician seems to have the advantage on the practical as well as on the aesthetic side. For what is useful above all is *technique*, and mathematical technique is taught mainly through pure mathematics.

Let us illustrate Hardy's thought in a typical example. Oftentimes, the time lapse between the initial idea and the subsequent discovery, and then between the discovery and its technical application, takes decades, or centuries. It would had been impossible to *discover* lasers in nature, they had to be *invented* on the basis of Quantum Mechanics. In turn, Quantum Mechanics could not have emerged without the preceding development of physics and mathematics, including, in particular, complex numbers, differential equations, or matrices.

However, the Italian XVI century algebraists, who introduced complex numbers, have done it for fun and for sport, rather than any practical applications. They have not been considering the possible role of complex numbers in Quantum Mechanics or lasers — or, for that matter, even in the alternating current or radio.

If you can summarise the XX century social and educational ideas with one word, that word would be "OVERSIMPLIFICATION". Yuri Manin [25] makes an incisive comment to this effect:

> The core intrinsic contradiction of the market metaphor (including the outrageous "free market of ideas") is this: we are projecting the multidimensional world of incomparable and incompatible degrees of freedom to the one-dimensional world of money prices. As a matter of principle, one cannot make it compatible with even basic order relations on these axes, much less compatible with non-existent or incomparable values of different kinds.
>
> In this respect, the most oxymoronic use of the market metaphor is furnished by the expression "free market of ideas".
>
> Only one idea is on sale at this market: that of "free market".

Similarly, "useful education" is trying to sell you only one idea: that of "usefulness".

4. Mathematics for the general public: sociology

Around 1905–1915 there were elite schools in St Peterburg, *Gymnasia*, whose students were studying Algebra from textbooks by Dmitry Grave, which *started* with the notion of field, complex numbers, and the like, and stopped short of Galois theory — that was his next textbook, for the University. Unfortunately, the mathematical awareness of the less privileged population strata was much lower than that.

Here is how Alexandre Borovik describes the corresponding choice nowdays, see [6], reiterated in [7]:

> Democratic nations, if they are sufficiently wealthy, have three options:

> (A) Avoid limiting children's future choices of profession, teach rich mathematics to every child—and invest serious money into thorough professional education and development of teachers.
>
> (B) Teach proper mathematics, and from an early age, but only to a selected minority of children. This is a much cheaper option, and it still meets the requirements of industry, defence and security sectors, etc.
>
> (C) Do not teach proper mathematics at all and depend on other countries for the supply of technology and military protection.
>
> Which of these options are realistic in a particular country at a given time, and what the choice should be, is for others to decide.
>
> I am only calling a spade a spade.

We do not immediately see, what it has to do with democracy — or wealth, for that matter — option (B) is not that much cheaper, after all. But the choice is obviously there, anyway.

In the 1990-ies one of us was teaching *Matematica generale* to a class of 200 economics and management students at the *Università commerciale Luigi Bocconi*. Then, he was shocked by the fact that in the same class there were students from *ragioneria*, who have never seen logarithms before, and other students from *liceo scientifico*, who were quite proficient with multiple integrals. In the last decades, Russia has rapidly evolved in the same direction, from option (A) to option (B), so that a similar lack of uniform preparation is now routine at some departments of our university. But again that was a social choice as much as an economic one.

What moderates the situation in Russia, and what makes recruiting excellent **Mathematics**[2] students relatively easy, is the system of specialised Physics and Mathematics Schools, operating in all major Russian cities, starting with Moscow, St Petersburg, Novosibirsk, etc. The first such schools were created by Andrei Kolmogorov, Dmitry Faddeev, Mikhail Lavrentiev and others some 60 years ago and they are still *by far* the best, the most functional, and the most efficient component of the whole Russian educational system. The *Presidential Liceum* 239 is for St Peterburg what *Lyceé Louis-le-Grand* is for Paris, with all social implications. See the recent paper by Nikolai Konstantinov and Alexei Semenov [23] for a detailed description of the principles, the history, and the current state of the Physics and Mathematics Schools.

However, all of our gut instincts suggest that the sharpest possible form of option (A) is the only correct answer. We do believe, that comprehensive and profound *universal* education in mathematics and exact sciences would be an excellent idea. It was never attempted before in the history of mankind, and we agree with Rokhlin [27] that:

> Somehow we feel intuitively that it would be good if our children and grandchildren were familiar with the logical culture, with the mathematical culture, if they could understand the exact sciences better.

[2]Well, actually, Mathematics *and* Computer Science, see `https://math-cs.spbu.ru/en/`

5. Mathematics for the general public: instruction

The present day elementary mathematics instruction is encumbered by an overly rigid tradition, and is not up to the requirements of the XVI century. It may sound too dramatic, but we strongly believe this is the case. The existing curricula are mostly oriented towards the development of [obsolete] computational skills and mechanical use of a small number of [outdated] standard algorithms.

In the past, such similar needlework was of undeniable value, but today the need for mass training in ancient craftsmanship looks suspicious. It is akin to extracting fire by friction: you may have to use it once in your lifetime — probably not! — but it would be stupid to practice it each and every day.

Of course, it's up to you, how far you are prepared to go. Do we have to memorise the multiplication table 100×100? What about 10×10? Our viewpoint is as follows. It is useful to understand the idea of long multiplication — to get a clear understanding of the relative size of numbers, that the decimal notation is logarithmic [— or to multiply two 8-digit numbers that nobody has multiplied before, to get some feel of probability]. But it is pointless to systematically practice this skill — none of today's schoolchildren will have to perform such operations manually, simply because any computing device makes it faster, in a more efficient and more reliable way.

5.1. Curricula

With respect to the actual inner architecture of mathematics, or its current applications, the choice of the subject matter in school curricula seems to be rather arbitrary and bizarre. Of course, in many cases such oddities have a historical explanation, sometimes more than one.

Thus, for instance, the prevalence of **trigonometry** is easily explained by the needs of ballistics, and navigation. Here is what Alexandre Borovik [7] writes in merit:

> It is worth to remember that in the first half of the 20th century, school mathematics curricula in many nations were dictated by the Armed Forces' General Staffs – this is why trigonometry was the focal point and apex of school mathematics: in the era of mass conscription armies, it was all about preparation for training, in case of war, of a sufficient number of artillery and Navy officers and aircraft pilots. With this legacy, we still cannot make transition to a more human mathematics.

That's obvious, and obviously true. However, it does not explain why trigonometry is being taught in such an antediluvian manner, WITHOUT COMPLEX NUMBERS.

Of course, all of school trigonometry becomes immediately obvious once you explain that addition formulas for cosine and sine are *precisely* multiplication formulas for complex numbers, in various national traditions this is called **Euler formula**, or **de Moivre formula**, whatever. The father of one of us (who was an electrical engineer) explained this to him at the age of 10–11 years within half an hour.

This is not how it is done at schools, however. Instead, a child is forced to learn by rote dozens of seemingly unrelated special cases, and nobody explains the true meaning of signs, etc., one just has to memorise all of it.

The venial explanation due to Henri Lebesgue [24], is that this is done OUT OF PURE SADISM, just to torment and humiliate the child. A much more sinister interpretation is articulated by Yuri Neretin [26], who believes this was done on purpose, as part of a market strategy to create a separate field of knowledge, *elementary mathematics*.

The business plan behind is roughly as follows:

- to use mathematics as a barrier and filter — the so called *entrance mathematics*, or *exam mathematics*.
- to create a market for private or semi-private educational services – preparatory courses, private tutors, and the like + the corresponding literature, sites, etc.

Further, Neretin also observes that since this new field of knowledge does not have any relation whatsoever to any other branch of mathematics, pure or applied, the person who has perfectly mastered *entrance mathematics* does not thereby acquire any knowledge or skill remotely useful in mathematics or science.

Imagine the kind feelings the poor children and their parents must share towards *that* sort of mathematics! What is much worse, many of them are induced to think, this crossbreed of military training, bookkeeping and penmanship is authentic mathematics!

5.2. False rigour and misguided proofs

In many cases educators insist on obsolete ways of teaching certain things. It is obvious to all mathematicians for more than half a century now that one aspect of the school curriculum that should be *completely* revised, is geometry. Such a reform will not eliminate geometry, but, to the contrary, enhance and invigorate it! In fact, most of the geometric proofs along Euclid's line, which schoolchildren have to memorise for the sake of PRESUMED RIGOUR, are either incomplete, or incorrect, or incomprehensible.

At the same time, we all know that the XVII century approach by de Fermat and Descartes removes all such difficulties, and makes the whole subject transparent, open-ended and useful. It was clear to every competent mathematician for 40–60 years that this is how geometry should be taught at a mass school. Let us quote Jean Dieudonné [14], who was an exuberant advocate of this approach:

> For the trained mathematician of today, it is a triviality that the fundamental theorems of Euclidean geometry (in any number of dimensions, by the way) are very easily derived from the concept of a vector space equipped with a positive definite quadratic form. Why shouldn't this method be made available (in two or three dimensions) to high school students instead of the incredible, apparently irrelevant dissections of triangles, where every step is made to appear to be a conjurer's trick?

Nothing has changed since.

What is worse, many of the alleged proofs in the school geometry textbooks — including most of the proofs on lengths, areas and volumes — are overtly fake or fallacious. There are passionate narratives to this effect in the books by Lebesgue and Grothendieck [24, 17]. In 1981 Rokhlin [27] mentions it casually, as a common knowledge:

> I went to high school (perhaps, it's still the same now), I was told what the area of a circle is. I was told that this is some sort of limit, and then something was written or was stated, and we got a formula for the area of the circle. What was said was difficult to understand then, but when I became a mathematician, it became totally clear to me, why it was so difficult to understand. IT WAS ALL SHEER NONSENSE.

Again, nothing has changed since.

5.3. Elementary mathematics

What annoys us most about hierophants of the so called "elementary mathematics", however, is their chicanery and hairsplitting. For us, trained as professional mathematicians, all of their discussions seem to be completely devoid of meaning, and extremely artificial.

Russian educational networks burst with messages of the following type. When you count, how many beer bottles are there in 3 boxes of 6 bottles each, should you muliply 3×6, or 6×3? It turned out, there is a sacral order, approved by a certain Areopagus some centuries ago, and they actually **lower grades** to the poor children who do it otherwise, even getting the right answer. Only that we could never memorise, which order of operations they consider correct.

Wu Hung-Hsi [33] describes this outrageous situation as follows:

> One of the flaws of the school mathematics curriculum is that it wastes time in fruitless exercises in notation, definitions, and conventions, when it should be spending the time on mathematics of substance. Such flaws manifest themselves in assessment items which assess, not whether students know real mathematics, but whether they could memorize arcane rules or senseless conventions whose raison-d'être they know nothing about.

At a later stage there comes all that fuss about staying real, all that harassment conserning "the domain of allowable values", and suchlike. As Felix Klein observes [22], the elementary mathematics of this sort is a late invention, not earlier than the last quarter of the XIX century. Before that the XVIII and XIX century classics were always working in the complex domain.

Yuri Neretin [26] concludes: THE ABOVE-MENTIONED SCIENCE CAUSES IN A NORMAL YOUNG MAN ONLY TEDIUM AND DISGUST, OR, WHAT IS INCOMPARABLY WORSE, TORPIDITY.

6. Mathematics for non-mathematicians: what it is

The situation with training other professionals at the university level is similarly disgraceful. Obviously, in many executive respects it is much less odious than the mass mathematical education. But in terms of teaching content it is dominated by an obsolete tradition, which oftentimes makes it even less meaningful.

Historically, these "higher mathematics" courses are just diluted (or, as Rokhlin designates it, "watered-down") early XX century courses for mathematicians. These courses start with the same sequences, series and limits, and then pass on to the same derivatives, integrals, differential equations, etc., dealed with in a sterile and perfunctory manner.

Calculus textbooks, when they attempt at proving anything, are full of direct mathematical mistakes anyway, see [30]. Only that "higher mathematics" textbooks are usually worse than that, since they remove all deeper theorems and mathematically interesting examples, making the leftovers unsavoury, boring and impossible to digest[3].

Traditional mathematics courses for non-mathematicians — not just the absolutely stale and futile calculus courses, but most of the archaic service mathematics courses in linear algebra, differential equations, probability theory and discrete mathematics – are also focused almost exclusively on the mechanical exercise of rudimentary computational skills, without any deeper understanding of the true structure of the subject, its applications, its current state, or wider context.

Let us give an illustration of how slavishly the textbooks of higher mathematics follow traditional courses for mathematicians. We were shocked by seeing in a mathematics textbook for *philosophers* trigonometric substitutions, derivation of the function $x \mapsto x^x$, and the like. We recognise that the IDEA OF FUNCTORIALITY and the chain rule themselves could be extremely useful for philosopers. But we do not see any use in teaching them specific *technical* tricks for calculation of derivatives and integrals, whose gist they won't be able to grasp anyway.

As in school, there is a lot of insistence on "foundations" and the false "rigour". One of such completely artifical roadblocks is the "theory of limits". The emphasis on limits creates conceptual difficulties for many students, and it is absolutely irrelevant both for exposition of analysis itself, and for applications[4]. Here is what Rokhlin [27] says:

> ...the limits are part of the course that is most difficult to understand, and, what is interesting, absolutely unnecessary. Differential calculus, integral calculus, and, in general, all the classical mathematics, to say nothing of the finite mathematics, can be easily explained without the

[3]What Peter Taylor [28] says of the school curriculum is even more applicable at the university level: "The secondary-school mathematics curriculum is narrow in scope and technical in character; this is quite different from the nature of the discipline itself".

[4]This discussion is not new either. Already "Lüshi Chunqiu" compiled not later than III century B.C. mentions that A TRUE SCIENTIST DOES NOT KNOW LIMITS.

limits. More than that, they are not needed there. They are an absolutely extraneous phenomenon, extraneous subject that has been introduced into this area by the people who wanted to build a proper foundation for analysis.

7. Proofs and other evidence

We believe that the teaching of mathematics to non-mathematicians should be completely reformed. We do not see, why it should stay a downgraded version of training of mathematicians, either as far as the subject matter, or as style.

7.1. Proofs in education

Traditionally, it is claimed that most results stated in the elementary courses must be accompanied by complete proofs. Such a viewpoint seems to us HOPELESSLY OUTDATED, UNREALISTIC AND HYPOCRITICAL.

As it happens, in most cases, the presence or absence of proofs does not influence the confidence of students in the results themselves. We believe that the primary role of proofs in lectures and textbooks for non-mathematicians amounts to the following:

- To convince the students that they correctly understand the statement.
- To clarify the purport of a statement and its connection with other statements.

In the training of professional mathematicians proofs may have also other functions:

- To drill general patterns of mathematical reasoning (induction, reduction, partition into cases, general position, specialization, ...) and standard techniques in a specific area.
- To develop a habit and taste for precise arguments as such, and to exercise the ability to distinguish assumptions, evidence and plausible guesses from well-established facts.
- As they say in Cambridge, to illustrate some of the tedium.

All of these goals *might* be pursued also when teaching non-mathematicians — with some moderation, though, especially the last one!

In many cases proofs in educational literature, especially long, badly structured and purely computational ones, merely *disorient* the student, hazing and alienating the meaning. In research papers, bad proofs are better than none, but in teaching it's the other way round.

7.2. Other evidence

What many mathematicians seem to ignore, is that there is nothing sacrosanct about the current ("modern") forms of mathematical expression. The ways how we organise and record our arguments are provisional and historically determined. For the purposes of education, our present day "proofs" are no better, than the ancient

Egyptian "proofs", or ancient Chinese "proofs", or ancient Indian "proofs" — or ancient Greek "proofs", for that matter, they are just *different*. And, more probably than not, our current standards of reasoning and exposition are as transitory as these older forms.

A traditional proof, even less so a formal proof, are not the only ways to understand a mathematical result, and even for a professional mathematician they are rarely *the* best ways. There are smart proofs that explain things, that make us wiser, and such proofs should be cherished.

But otherwise to understand a statement you should look at examples, special cases, corollaries, experiments, heuristic arguments, analogies, applications, visualisation, etc. — this will usually tell you more about the true nature of a mathematical result, than most proofs. Much more so for students!

Just 100–150 years ago many mathematicians would *claim* that they verify the proofs of all results they quoted[5]. Today, a similar claim would sound pathetic. We have to rely always more on the work of others, and that's a one-way road. It is inevitable that we distribute our trust, see [9]:

> In all these settings, modern computational tools dramatically change the nature and scale of available evidence. Given an interesting identity buried in a long and complicated paper on an unfamiliar subject, which would give you more confidence in its correctness: staring at the proof, or confirming computationally that it is correct to 10,000 decimal places?

It is ridiculous to pretend that the students can meet the standard we have long abandoned ourselves.

8. Mathematics for non-mathematicians: what should we teach, really?

Our short answer to the question in the section heading is: WE DO NOT KNOW — and nobody does! There are several possible answers, the following most immediate ones:

- The same as always — whatever, limits, eigenvalues, ...
- What is used in the corresponding subject field today — well, between "the same as always", and "nothing".
- Nothing — no joke! This viewpoint has more and more supporters!
- The mathematics of mathematicians.

Our answer is that we should teach mathematics as we, mathematicians, understand it. What we think important — the language, some general concepts that would allow to assimilate further concepts, and, above all, the mathematical thinking itself: basic techniques, some most productive arguments and ways of reasoning, some classical constructions, etc.

---

[5]Whether they were actually doing that, is a completely different story. We bet, not [30].

As far as the subject matter, it is our belief that it does not matter much, what exactly we teach. Nobody knows what exactly will be used in a specific field — certainly we do not know, but, as we said, nobody does.

We believe that the only way for the science and technology to advance, is to expose the professionals in these fields to more mathematics, more advanced mathematics — and, above all, meaningful mathematics, both classical and modern. But to do it *differently*, focusing on conceptual aspects, **understanding**, applications, rather than on technical details of the proofs or specific computational skills.

It's not that they should stop studying mathematics relegating all computations to computers instead — quite to the contrary, they should be exposed to richer and deeper mathematics.

9. Mathematics and computers

We have already quoted, on several occasions, the following observation by Doron Zeilberger [34]:

> The computer has already started doing to mathematics what the telescope and microscope did to astronomy and biology.

We cannot agree more! In fact, we are convinced that mathematicians today have better access to the mathematical reality, than most experimental sciences have to physical reality, see [20, 31]. And we tend to agree with Borovik [8] that the current ineffectiveness of Mathematics in Biology and other applications *might* be explained by the fact that the requisite Mathematics is simply too large for an individual human mind.

9.1. Mathematics for end-users

Computers have *already* completely redefined the applications of mathematics, the way in which mathematics will be handled in any predictable future by most end-users. We should be completely honest with ourselves that *none* of our students will *ever again* solve a system of linear equations, invert a matrix, calculate an integral or graph a function *by hand*, outside of the mathematics class. Why should we insist that they do it without the use of *computing machines* in the mathematics class?

They say that the mother of Carl Friedrich Gauß could observe with the naked eye phases of Venus and some moons of Jupiter. Unfortunately, for the vast majority of the usual people this is not possible, they have to resort to the help of *magnifying machines*.

This is clear to the end-users in the corresponding fields, as this is absolutely clear to our students. But we still prefer to pretend that we are doing something useful by feeding them badly chewed cardboard, which they do not need, and cannot digest anyway. As a result, many end-users start to complain, louder and louder.

In the last years, we've heard from more than one engineer, and not some imposters, but rather serious professionals, that there is no need to teach mathematics to [all of] engineering students anymore, just computers. We know they are wrong and that even the present day imperfect and retarded mathematical instruction is better then none. And a real sensible course of conceptual mathematics — **mathematics of mathematicians** would start a Golden Age in some subject fields. But at the end of the day, they will decide!

9.2. Mathematics for players

There is another closely related aspect, which we do not touch here, and which will eventually change the scene completely.

Most mathematicians tend to dramatically underestimate to which extent the development of mathematics is determined by the external circumstances, in the first place by the available computational resources. But whether we appreciate it or not, mathematics itself is in the process of an immense metamorphosis, one of the greatest in its history.

Already today the progress of computers and Computer Algebra Systems strongly influences research in many areas of pure mathematics itself — such as group theory, combinatorics, number theory, commutative algebra, algebraic geometry, etc. Predictably, in the nearest future this influence will expand to all of pure mathematics and will produce *Umwertung aller Werte*: radical revision of research directions and style.

10. Existing Computer Algebra Systems

For us, it is obvious that teaching science and engineering students to calculate derivatives and integrals, to solve algebraic or differential equations, to multiply or invert matrices by hand, or the like, is a sheer waste of time. These skills are as osbolete as the use of a slide rule or a logarithm table.

As of today, the *default* tools for all these things are the **general purpose CAS** = Computer Algebra Systems.

• There are a huge number of elementary low-end products with limited functionality, used at the elementary stages of teaching mathematics, at the level of elementary and secondary schools. Some of them, such as `MathCad`, are essentially text editors, not much different in their functionality from `Excel`. Some others are quite useful, interesting and funny, but none of them is vertically integrated or systematically expandable by the end-user. Thus, they cannot be used in teaching any serious mathematics at the university level.

• There are also many **specialised CAS**, which are simply *fantastic* at doing some things, such as polynomial calculations, or linear algebra, but do not cover the full range of symbolic mathematics. Of course, there are a huge number of extremely flexible and powerful specialized systems, such as `GAP`, `Magma`, `CoCoA`, `Singular`, `Pari`, `Lie`, etc., specially created for computing in specific areas such as number theory, group theory, representation theory, commutative algebra, algebraic geometry, etc.

What is essentially missing is the intermediate sector, general purpose Computer Algebra Systems covering a wide range of different branches of mathematics at the high intermediate level.

• Dropping the systems that are experimental, obsolete, not powerful enough, not supported anymore, too complicated or too expensive, do not have convenient Front End, or do not support graphics, you are left with an amazingly limited choice, essentially only four products: `Axiom`, `Maple`, `Mathematica`, and `SageMath`.

All of these four systems are VERY VERY GOOD. All of them are, in the first place, very high-level programming languages, whose expressive power approaches fragments of a natural language. All of them can perform *all* usual computations, anything that a non-mathematician is likely to see in *any* possible present day application.

Nowadays, teaching top end computer scientists or mathematicians we would *probably* choose `Axiom` and `SageMath`, with some reservations. Purely mathematically, as far as its expressive power, `Axiom` might be the most interesting Computer Algebra System of all. However, after the death of its creator Richard Jenks, `Axiom` was for a long time not supported, and has not developed convenient intuitive front-end. To the contrary, `SageMath` is actually not an independent system, but a convenient front-end that provides a qualified user with access to several dozen specialised systems.

Thus, for a number of reasons, teaching non-mathematicians you have to choose between `Maple` and `Mathematica`, which is purely a matter of taste. In our courses we used *both*, but for a number of *extra-mathematical* reasons eventually opted for `Mathematica`.

11. The course "Mathematics and Computers"

In 2005 we started to teach a two-semester course "MATHEMATICS AND COMPUTERS" at the Economics Department of St Petersburg State University, the Spring semester of the 1st undergraduate year + the Fall semester of the 2nd undergraduate year.

For administrative reasons[6] the second semester of this course was sometimes called "MATHEMATICAL SOFTWARE", but it was a direct sequel of the same course anyway, so that one should think of our course as "Mathematics and Computers, I" and "Mathematics and Computers. II".

[6] The absurd bureaucratic requirement that courses in different semesters should have different names.

The course was taught not to all economics students, just to those specialising in "MATHEMATICAL METHODS IN ECONOMICS"[7] and in "APPLIED INFORMATICS IN ECONOMICS"[8], about 25 students per year each, 50 students per year total.

Another person actively involved in the development of this project at the initial stage was Oleg Ivanov. Later he and Grigory Fridman have launched a similar project at the St Petersburg State University of Economics and Finance, see [19], for instance.

A normal class was mixed format. It usually started with introducing some new mathematical concepts and ideas, and a few key statements with occasional proofs. The proofs were only explained when they were especially short and transparent and contained powerful general ideas which work in many situations. After that we gave suggestions for further reading, for those who wanted to study these concepts deeper and passed to algorithms and computer demonstrations, computations, graphics, etc. After that we distributed small standard problems and larger semi-research projects, both individual and for small groups of 2–3 students. Both were subsequently discussed in the class, very selectively, though, sometimes only in case of difficulties, otherwise only answers, ideas, and/or parts of the code.

The course would concentrate on basic mathematical ideas, rather than specific applications. Below we list the topics which were covered sort of each year. Otherwise, we allowed a lot of flexibility and any given year could mention different examples and subject fields.

12. Some tapas of Computer Algebra

We would usually start our class with a dozen or so demonstrations, of what is mathematics, really, and how computer can help. The actual examples would vary each year, below we reproduce some typical computations we were showing to our students at the first lecture, as a warm up for our course.

12.1. Elkies counter-example

Obviously, our students heard of Fermat problem. So we asked them whether they heard that Euler suggested a broad generalisation of that. Namely, he claimed that for $m \geq 4$ the equation

$$x^m + y^m + z^m = u^m$$

does not have solutions in natural numbers. That for $m \geq 5$ the equation

$$x^m + y^m + u^m + v^m = z^m$$

does not have solutions in natural numbers, etc.

However, in 1988 Noam Elkies [15] discovered that

$$2682440^4 + 15365639^4 + 18796760^4 = 180630077292169281088848499041 = 20615673^4.$$

[7] This major was created at St Petersburg State University in the 1930-ies, by Leonid Kantorovich.

[8] This major was relatively new, and only created in the early 2000-ies. Presently it changed the name to "BUSINESS INFORMATICS".

Of course, finding such a solution with a home computer without knowing some rather advanced algebraic number theory and algebraic geometry is not feasible.

However, a similar counter-example for the fifth powers

$$27^5 + 84^5 + 110^5 + 133^5 = 61917364224 = 144^5$$

can be found by any student by brute force, within a few hours.

12.2. Ramanujan for low-brows

Polynomials can tell you many stories as well. Let us reproduce the famous 6-10-8-Ramanujan identity, see [5]. Set

$$\begin{aligned} f_n(x,y) = (1+x+y)^n + (x+y+xy)^n - \\ - (1+x+xy)^n - (1+y+xy)^n + (1-xy)^n - (x-y)^n \end{aligned} \quad (1)$$

Then

$$64 f_6(x,y) f_{10}(x,y) = 45 f_8(x,y)^2$$

Of course, we would demostrate this by brute force, simply by opening all brackets and evaluating both sides to

$$46080x^2y^2 + 322560x^3y^2 + 887040x^4y^2 + 1128960x^5y^2 + 241920x^6y^2 - \ldots$$

Ramanujan identities are in a sense most peculiar, since even for a mature mathematician it is not always easy to guess what goes on inside. But otherwise usually any of the Liouville identites, or even the corollaries of the Newton—Waring identities suffice to impress a student.

12.3. High precision fraud

We would usually show a couple of examples illustrating the difference between the mathematical and computational viewpoints, and the need for infinite precision calculations.

For instance, $e^{\pi\sqrt{163}}$ is so close to being an integer, that even the calculation with 12 positions after the decimal point still does not allow to tell, whether it's integer, or not

$$262537412640768743.999999999999$$

Of course, this only looks weird. Every competent mathematician knows that there is an obvious explanation, consisting in the fact that $\mathcal{O}_{-163}$ is a principal ideal domain. The numbers $e^{\pi\sqrt{67}}$ and $e^{\pi\sqrt{43}}$ are also very close to integers, though not with such marvellous precision.

12.4. BBP-formulas

Another highlight of Computer Mathematics is the formula which allows to compute any *hexadecimal* digit of π separately, without computing the previous ones, see [2, 3]:

$$\pi = \sum_{k=0}^{\infty} \frac{1}{16^k}\Big(\frac{4}{8k+1} - \frac{2}{8k+4} - \frac{1}{8k+5} - \frac{1}{8k+6}\Big).$$

12.5. Inverting a 1000×1000 matrix

As another *tapas*, we would generate a random real 1000×1000 matrix, with values in the range, say $[-10, 10]$, machine precision. And then invert it, machine precision, which would normally take 3–4 seconds. Then we would comment that the amount of numerical computation involved in this individual evaluation far exceeds all numerical computation that all students in the class will perform, or could possibly perform, during their life-time.

Usually, the students were shocked, excited and amazed. We told them we could not teach them *discover* such things, but within a year or so we can certainly bring them closer to understanding and appreciating some of the mathematics behind such examples, and perform such similar calculations — and in fact *all* usual calculations! — with confidence. Thereafter, we usually had their attention.

We do not know, how to teach students who are not impressed by this kind of examples. It is our belief that in such extreme cases any medicine is powerless. As observed at the very beginning of the treatise [11] by Nicolas Bourbaki:

> Nous ne discuterons pas de la possibilité d'enseigner les principes de mathématique à des êtres dont le développement intellectuel n'irait pas jusqu'à savoir lire, écrire et compter.

13. Borwein's joke

Here is a similar (fancier!) example we were not showing to our students. But next time we certainly will! Consider the following sequence of integrals, see [10]:

$$\int_0^\infty \frac{\sin(x)}{x}\,dx = \frac{\pi}{2},$$

$$\int_0^\infty \frac{\sin(x)}{x}\,\frac{\sin(x/3)}{x/3}\,dx = \frac{\pi}{2},$$

$$\int_0^\infty \frac{\sin(x)}{x}\,\frac{\sin(x/3)}{x/3}\,\frac{\sin(x/5)}{x/5}\,dx = \frac{\pi}{2},$$

$$\int_0^\infty \frac{\sin(x)}{x}\,\frac{\sin(x/3)}{x/3}\,\frac{\sin(x/5)}{x/5}\,\frac{\sin(x/7)}{x/7}\,dx = \frac{\pi}{2},$$

$$\int_0^\infty \frac{\sin(x)}{x}\,\frac{\sin(x/3)}{x/3}\,\frac{\sin(x/5)}{x/5}\,\frac{\sin(x/7)}{x/7}\,\frac{\sin(x/9)}{x/9}\,dx = \frac{\pi}{2},$$

$$\int_0^\infty \frac{\sin(x)}{x}\,\frac{\sin(x/3)}{x/3}\,\frac{\sin(x/5)}{x/5}\,\frac{\sin(x/7)}{x/7}\,\frac{\sin(x/9)}{x/9}\,\frac{\sin(x/11)}{x/11}\,dx = \frac{\pi}{2},$$

$$\int_0^\infty \frac{\sin(x)}{x}\,\frac{\sin(x/3)}{x/3}\,\frac{\sin(x/5)}{x/5}\,\frac{\sin(x/7)}{x/7}\,\frac{\sin(x/9)}{x/9}\,\frac{\sin(x/11)}{x/11}\,\frac{\sin(x/13)}{x/13}\,dx = \frac{\pi}{2}.$$

Guess the value of the next one.

Well, actually the pattern breaks at the next step:

$$\int_0^\infty \frac{\sin(x)}{x}\,\frac{\sin(x/3)}{x/3}\,\frac{\sin(x/5)}{x/5}\,\frac{\sin(x/7)}{x/7}\,\frac{\sin(x/9)}{x/9}\,\frac{\sin(x/11)}{x/11}\,\frac{\sin(x/13)}{x/13}\,\frac{\sin(x/15)}{x/15}\,dx =$$

$$\frac{467807924713440738696537864469}{935615849440640907310521750000}\pi.$$

The reason is of course that

$$\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{9}+\frac{1}{11}+\frac{1}{13} < 1, \quad \text{but} \quad \frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{9}+\frac{1}{11}+\frac{1}{13}+\frac{1}{15} > 1,$$

and it's a [highly non-trivial!] exercise in harmonic analysis and integral transforms to work out what goes on here! There are more such remarkable examples, see [1, 13, 21] and references there.

14. Actual curriculum of the course "Mathematics and Computers"

Usually, we started with warm up material on subjects which were [partly] familiar to many of the students — but not to all of them! Part of the idea was that the students begin facile coding with topics where mathematics is either familiar or amusing [or both!], and feel some initial confidence.

- **Arithmetics**. We started with integers, rational numbers, real and complex numbers, and modular arithmetics. Various formats, basic algortihms, elementary functions, calculation of powers, Euler formula and de Moivre theorem, roots of 1, congruences up to, say, Euclidean algorithm, finite fields and Chinese Remainder Theorem. Sometimes this part included some fancier topics, like continuos fractions, denesting of radicals, harmonic numbers, Bernoulli numbers, etc.
- **Basic number theory**. That would normally include primes, Eulcid's theorem and the Fundamental theorem of Arithmetics, some dainties like Fermat and Mersenne primes, the prime number theorem and Dirichlet theorem on

primes in arithmetic progression[9], Fermat and Euler theorems, pseudoprimes, Legendre symbol, quadratic reciprocity. We would mention also some classical problems in additive number theory, but no part of that was required for the exam, it served only as a source of research projects in the style of recreational mathematics.

The part on discrete mathematics and combinatorics was the central part of the course, at least the focus of the 1st semester, in view of the fact that we were teaching prospective high-end computer users.

- **Combinatorics I**. That would normally include factorials, raising and falling factorials, binomial and multinomial coefficients, Stirling and Bell numbers, Catalan numbers, generating functions, and the like. Here, we would present as many proofs as possible, to practice such ideas as induction, partition into cases, Dirichlet principle, recurrencies, etc.
- **Discrete Mathematics I**. Lists: generation of lists, parts of a list, basic structure manipulations, nested lists, trees and other data structures, various algorithms for sampling, search and sorting. Sets and multisets: subsets, chains and antichains, Boolean operations, Cartesian products, enumeration theory, inclusion-exclusion, partitions, Gray code.
- **Discrete Mathematics II**. Maps: functions, Dirichlet principle, surjective and injective maps, pure and anonymous functions, λ-calculus, compositions and iterations, orbits, trajectories, and fixed points. Relations: Binary relations, graphs, equivalence relations, order relations, Hasse diagrams, Möbius inversion, Ramsey theorem, Hall theorem (with proofs!)
- **Combinatorics II**. Permutations: algebra of permutations, symmetric group, generation of permutations, lexicographically and otherwise, transpositions, change ringing, sign of permutations via decrement and inversions (with proofs!), alternating group, involutions. Cycles: canonical decomposition, long cycles, multiplication of cycles, cycle type and conjugacy classes, statistics of cycles, maximal order, and the like.

That would normally take most of the first semester, after which most students would feel quite confortable in translating mathematical problems into fully functional code in `Mathematica`, and eager to apply this skill to other fields of mathematics which they studied.

The end of the first semester, and the beginning of the second semester were a medley of further basic mathematics and [mathematical] applications. Here, we would normally cover some further basic constructions, and various somewhat deeper topics.

Typically, this material would start with the two following classical constructions, with some proofs (but by far not all of them!)

[9] Both without the faintest sketch of proof, just as experimental facts! The students had to verify them up to certain limits and in certain special cases as experimental facts.

- **Polynomials**. Structure manipulation with polynomials, rational functions, power series, and the like, coefficients, roots, effective evaluation, fast multiplication and division, convolution, various flavours of interpolation (Newton, Taylor, Lagrange, Hermite,...), fast Fourier transform, algebraic equations and factorisation of polynomials, Gauss theorem, Chebyshev polynomials, cyclotomic polynomials, classical orthogonal polynomials, etc. Polynomials in several variables, symmetric polynomials (Viète, Newton, Waring,...), etc.
- **Matrices**. Structure manipulations with rows, columns, matrices and other tensors, parts of a matrix, multipication of matrices and other operations, matrices and linear maps, eigenvalues and eigenvectors, various notions of rank, elementary transformations, systems of linear equations, inverse matrix, various classical types of matrices (symmetric, orthogonal, circulant, etc.), block matrices and efficient algroithms, Kronecker product and sum of matrices, determinants and other invariants, canonical forms.

As applications we would usually mention some further topics, discussing them very briefly in the class, and offering all more complicated themes as projects for homework (at this stage it was assumed that the students spend *at least* 3 homework hours for each class hour).

- **Calculus**. Derivatives, integration, differential equations, whatever.
- **Linear Algebra**. Aplications to geometric and/or applied problems of linear algebra.

In the second semester, we would also discuss the topics required to produce a document containing complex mathematical formulas and computations, and, maybe something else, text, graphics, and other elements.

- **Algorithms with strings**. Transformation of text, formulas and tables: search, sorting, formatting, etc., rudimentary typesetting issues.
- **Basic Graphics**. Graphs of functions of one and two variables, geometric transformations of objects in 2 and 3 dimensions: translations, rotations, symmetries. Usually up to, say, regular and semi-regular solids, tilings and wallpaper groups.

This was a rather intensive course, and we do not believe we could do much more than that within a year at such an early stage, given the preparation of the students, and the share of their time they could devote to our course.

15. Can this project be scaled?

Overall, we judge this project as a complete and overwhelming success. It was certainly a refreshing and gratifying experience for ourselves. Much more fun than teaching the usual service courses anyway!

With active participation and interest on part of students we succeeded in covering much more Mathematics, more varied Mathematics, more interesting and useful Mathematics, with much better results, than would ever be possible with more traditional approaches.

It was, as we know, quite an experience for our students, many of whom later indicated that as a result of our course they understood what mathematics was about, stopped being scared by mathematics, started to love formulas, numbers, graphs, and as a result routinely use specialised mathematics tools for other courses.

Whether a similar project is portable and would be equally successful at a different university and/or within a different subject field, is not quite clear to us. We believe this is necessary, but should be addressed with caution.

In fact, we fully realise that here at the St Petersburg State Univ. we were in a privileged position in more than one respect.

1. It is one of the two universities in Russia (the other one being the Moscow State Univ.) that enjoy full academic autonomy. We can introduce new courses without any authorisation or approval of the Ministry of Science and Higher Education, or any other administrative body.
2. The project had full support of the Dean's office, both administrative, and financial. We had to present the course at the Teaching committee and the Departmental council, but essentially we had free hand as far as its outline and contents.
3. We had *two* fully equipped computer classes, with blackboards and 25+1 computers joined to a local network, with licenced copies of `Mathematica`, `Maple` and other necessary software installed + friendly technical support.
4. The programs "Mathematical Methods in Economics" and "Applied Informatics in Economics" are fairly competitive and select [mostly] good students, who were prepared to work with computers anyway. Many of them had preceding experience of programming in low level languages.
5. Many of these students were coming from good St Petersburg schools and had previous exposure to some calculus, vector analysis and the like at school, others were taking traditional courses of calculus and/or linear algebra in parallel.
6. Virtually all of the students had home computers with *some* mathematical software, and full access to the departmental computers with licensed copies of `Mathematica`, `Maple`, etc., outside of the class hours.
7. Most of the students had good working command of English, so that we did not have to translate for them help files, problems, instructions, jokes, etc.

Obviously, any of these points could break even at an equally excellent university, and all of them will break if you consider passage to lower level education.

In fact, it is not feasible that every school class could be equipped with comparable hardware, to install licenced commercial CAS such as `Mathematica`, `Maple` or `Axiom`. One of the points to start should be creation of a simpler and less demanding CAS with front end in national languages.

16. Our conclusions concerning teaching of non-mathematicians

Below, we outline our general convictions about teaching mathematics to non-mathematics students, summarising a few decades on teaching experience.

1. Teaching of Mathematics for non-mathematicians must be fascinating, vivid, inspiring. It is much more important to demonstrate the beauty and power of Mathematics, than to teach any specific topic. Mathematics is fun, any teaching that ignores this basic fact is harmful in times of peace, and dangerous in wartime.
2. The choice of specific content is mostly immaterial, since we do not know what kind of mathematics they will use during their careers anyway. The mathematical culture, the mathematical way of thinking themselves, positive attitude and willingness to study new topics and to use Mathematics are way more important.
3. The value of most of specific computational skills is negligible. Most of the students will never use these skills during their careers. Most of the specific calculations will be relegated to a computer, and difficult cases require professional advice anyway. Conceptual understanding and awareness are by far more valuable.
4. Most of the proofs have subordinate value. The student can understand a mathematical concept or result and sensibly use it without knowing the proofs. In most cases examples, special cases, corollaries, applications, analogues, experimental data, visualisations can do as much or more to explain a result, than a formal proof.
5. Computers have dramatically changed applications of mathematics. But computers have not made Mathematics obsolete. They have made obsolete only the current teaching of mathematics that was obsolete anyway, even before the advent of computers. Quite to the contrary, today we have to teach most professionals more Mathematics, more profound Mathematics, more advanced Mathematics, but we have to do it differently.
6. If you cannot beat them, join them. We have to welcome symbolic calculations and Computer Algebra Systems in mathematics class, and widely use them as a medium of instruction. Of course, the corresponding conversion of all mathematical courses, curricula, tests, exams, etc. will require a lot of work. But if done right it entails no dangers for mathematical education, just possibilities.

To finish on a slightly more cheerful note, let us quote Asterix:

> Gauls! We have nothing to fear; except perhaps that the sky may fall
> on our heads tomorrow. But as we all know, tomorrow never comes!!

Tomorrow does come. It is *almost* there. Our only hope is that its arrival is leisurly enough to give us, the mathematical community, time to adapt and reform the teaching of mathematics before it is too late.

17. Computer Mathematics at large

Speaking about the role of computers in mathematics, many people limit themselves, on the one hand, to the role of *numerical* calculations in applications and, on the other hand, to systems of formal inference (automatic theorem proving, formal verification of proofs, etc.). In these directions, especially in the first one, there are well-established schools and serious achievements in Russia.

In our view, Computer Mathematics is far from being reduced to these two subfields. In particular, in the near future, systems of **symbolic computation** and, in particular, **Computer Algebra Systems** will acquire much greater importance both for mathematics itself and for its applications.

In particular, in recent years it has become clear that for many real world industrial projects, not the traditional applied mathematics and numerical methods are in demand, but various areas of fundamental mathematics and advanced computer technologies.

There are also strong research groups in these areas, especially in Dubna, Moscow and St. Petersburg, they have extensive experience in creating Computer Mathematics tools tailored to perform special types of calculations for specific applications, usually in mathematics itself, physics and astronomy, partly engineering.

However, the functions implemented in these tools are usually rather specialised, limited to a specific problem, and do not even cover sufficiently broad areas of mathematics. Thus, these packages themselves cannot be directly used in general mathematical education.

In addition, in Russia, among mathematicians themselves, there is a *widespread distrust* of the capabilities of symbolic computing systems, it is customary to point out "errors in Computer Algebra Systems". From our viewpoint, predominantly all such "errors" are absolutely fictitious and are associated, on the one hand, with misunderstanding of the basic principles of computer calculations, and, on the other hand, with the objective difficulties of interpreting their results in traditional mathematical terms.

It should be honestly admitted that in this respect Russian mathematics visibly lags behind the world level.

18. The need for a new Computer Algebra System

18.1. `Mathematica` and `Maple`

As we mentioned in § 10, there are very few full-fledged general purpose Computer Algebra Systems = general purpose CAS, that can be used in education.

Two of these systems, `Mathematica` and `Maple`, are commercial. These are absolutely wonderful, great software products that, at the time of their creation in the 1980s, represented an outstanding achievement in Computer Mathematics and became the de facto standard for organizing such systems.

On the other hand, some fundamental decisions regarding their general architecture, organization of calculations, data structures, etc., taken at that moment, later turned out to be impossible to change, precisely due to the commercial nature of the systems and the need to ensure backward compatibility.

In addition, changes in the latest versions of these systems are increasingly focused not on aspects that are important from the point of view of mathematics itself, but on various purely marketing points: various specific extra-mathematical applications, computer graphics, music, animation, etc.

Unlike the `Axiom` system, both of these systems do not have simple and natural language tools for describing mathematical structures in terms of axioms or properties. Some extremely important mathematical constructions (symbolic polynomials, symbolic matrices, etc.) were included in them only post factum, with not the most efficient algorithms.

18.2. What has happened since?

However, over the past 30–40 years there has been tremendous progress in understanding the principles of Computer Mathematics. At present, it has become ideologically and technically possible to create systems whose language, in terms of vocabulary and expressive power, is much closer to the language actually used by mathematicians (= human mathematicians).

• Such a language should make it possible to describe mathematical structures in a way that is actually done in mathematical books (with a slightly more rigid syntax). This would allow, in particular, to implement the front-end of such systems in any national language.

• In addition, in many cases, more efficient algorithms and methods for organizing calculations have been proposed that allow calculations to be carried out faster and using less resource. In particular, parallel algorithms that were not used in traditional CAS have received significant development.

• Functional quantum computers do not yet exist, despite numerous declarations in this direction. Nevertheless, we are convinced that already today it is necessary to develop quantum algorithms of Computer Algebra and train specialists in this field. Traditionally, one only addressed issues of accelerating numerical computations. However, quantum algorithms could equally dramatically accelerate symbolic computations. It could be said that the presence of fast quantum algorithms makes it possible to consider **Post Quantum Computer Algebra** as a separate topical area of research.

• Over the past decades, the difficulties of translating the results of symbolic calculations into the language of traditional mathematics have been much better understood and, to a large extent, overcome.

18.3. Our project towards creation of a next-generation CAS

This feeds rather realistic expectations for the possibility of creating a *modern* symbolic computing system with the internal language and expressive power much closer to the traditional mathematical language. The results of computation in such a system would be much easier to interpret in traditional mathematical terms. In particular, such a system could easily afford front-end in any natural language, specifically in our case, in English *and* Russian (and the next option we would consider, is, of course, Chinese).

Such a system could be vertically integrated and, on the one hand, according to the requirements for equipment and user qualifications, accessible even to schoolchildren, and on the other hand, allow very sophisticated mathematical applications that are interesting to professional mathematicians.

In addition to the actual scientific interest, the creation of a system would become an essential element both in scientific research, also outside mathematics, and would be of great importance for mathematical education at various levels.

Preferably, such a system should be open (open-source), with a clear separation of the core, libraries of algorithms, supporting various areas of modern pure and applied mathematics, a developed data type system that allows, at the language level, to construct objects of new types using language constructs as close as possible to the language of modern mathematics, as well as various interfaces with the ability to modify parts of the code by a qualified user.

We have started to work towards creating front-end software that would provide support for cloud computing, parallelisation of algorithms, as well as interfaces for interacting with other Computer Algebra Systems, such as `Mathematica`, `Maple`, `Wolfram Alpha` and others.

We would have in mind the availability of such a system for use at all levels of mathematical education in Russia and, potentially, in other countries, from secondary schools to the training of professional mathematicians.

In a sense, the newest and least technologically developed here would be precisely the intermediate level, i.e. teaching mathematics to non-mathematicians: both engineers, physicists, chemists, biologists, and representatives of economic disciplines, and humanities

In cooperation with the colleagues from St. Petersburg, Moscow, Dubna and Canada we have started preliminary planning and research towards developing such a system. Our initial ambition is to create a Computer Mathematics Lab at the Department of Mathematics and Computer Science of the St Petersburg State University primarily dedicated to the development of the architecture, and preliminary design of such a system, and the study of various related scientific, technological, and educational issues.

Of course, an actual creation of such fully functional CAS along these lines would be an extremely ambitious project, that would require coordinated effort of dozens of people, both mathematicians, and computer scientists, over many years.

Acknowledgements

A major inspiration for us were numerous discussions with Sergei Pozdniakov and Alexei Semenov on the educational aspects of this work, and with Arsen Khvedelidze, Alexei Semenov, Alexander Tiskin and Nikolai Vasiliev on the current state and prospects of Computer Mathematics in general, and specifically of various aspects of symbolic computation. We thank Vladimir Kondratiev for his valuable technical support. Also, we thank Grigory Fridman, Boris Kunyavski and Alexander Merkurjev for very careful reading of our original manuscript and important corrections.

A tribute

In the previous list of acknowledgements, two key persons are missing. Over the last two years, we lost two great masters, Oleg Ivanov, who was instrumental in advancing computers into mathematical education, and Vladimir Gerdt, who was maybe the most knowledgeable expert in all aspects of computer mathematics and its applications. We very much miss them, their keen judgement and advice.

References

[1] D. H. Bailey, J. M. Borwein, *Experimental mathematics: examples, methods and implications*, Notices Amer. Math. Soc.,**52** (2005), no. 5, 502–514.

[2] D. H. Bailey, J. M. Borwein, P. B. Borwein, S. Plouffe, *The quest for* `Pi`. Math. Intelligencer, **19** (1997), no. 1, 50–57.

[3] D. Bailey, P. Borwein, D. Plouffe, *On the rapid computation of various polylogarithmic constants*. Math. Comput., **66** (1997), no. 218, 903–913.

[4] H. Bass, *Mathematics, mathematicians, and mathematics education*. Bull. Amer. Math. Soc., New Ser. **42** (2005), no. 4, 417–430.

[5] B. C. Berndt, S. Bhargava, *Ramanujan for low-brows*, *Amer. Math. Monthly*, **100** (1993), 644–656.

[6] A. V. Borovik, *Calling a spade a spade: Mathematics in the new pattern of division of labour*, In Mathematical Cultures: The London Meetings 2012–14 (B. Larvor, ed.). Trends in the History of Science. Springer, 2016, 347–374. ISBN 978-3-319-28580-1. DOI 10.1007/978-3-319-28582-5_20.

[7] A. V. Borovik, *Mathematics for makers and mathematics for users*, In Humanizing Mathematics and its Philosophy: Essays Celebrating the 90th Birthday of Reuben Hersh (B. Sriraman ed.), Birkhauser, 2017, 309–327. DOI 10.1007/978-3-319-61231-7_22. ISBN 978-3-319-61231-7.

[8] A. Borovik, *A mathematician's view of the unreasonable ineffectiveness of mathematics in biology*. Biosystems, **205** (July 2021), 104410, `https://doi.org/10.1016/j.biosystems.2021.104410`

[9] J. M. Borwein, *Implications of experimental mathematics for the philosophy of mathematics.* In Proof and Other Dilemmas: Mathematics and Philosophy. Providence, RI: Amer. Math. Soc., 33–61, 2008.

[10] D. Borwein, J. M. Borwein, *Some remarkable properties of sinc and related integrals*, The Ramanujan Journal, **5** (2001), no. 1, 73–89.

[11] N. Bourbaki, *Éléments de mathématique. Tous les 28 tomes, y compris le dernier tome Topologie Algébrique Chapitre* 1–4. 2017, Berlin: Springer, 7902p., ISBN 978-3-662-53102-0/pbk.

[12] D. M. Bressoud, *Is the sky still falling?* Notices Amer. Math. Soc. **56** (2009), no. 1, 20–25.

[13] A. D. Burazin, V. Jungić, M. Lovric, *A cultural challenge: teaching mathematics to non-mathematicians.* Maple Trans. **1** (July 2021), no. 1, Article 14144, 11p. `https://doi.org/10.5206/mt.v1i1.14144`

[14] J. Dieudonné, *Should We Teach "Modern" Mathematics?* American Scientist, January-February **61** (1973), no. 1, 16–19.

[15] N. D. Elkies, *On* $A^4 + B^4 + C^4 = D^4$. Math. Comput., **51** (1988), 825–835.

[16] S. A. Garfunkel, G. S. Young, *The sky is falling.* Notices Amer. Math. Soc. **45** (1998), no. 2, 256–257.

[17] A. Grothendieck, *Recoltes et semailles. Réflexions et témoignage sur un passé de mathématicien*[10]. 1986, 929p. `https://jmrlivres.files.wordpress.com/2009/11/recoltes-et-semailles.pdf`

[18] G. H. Hardy, *A mathematician's apology.* With a foreword by C. P. Snow. Reprint of the 1992 edition. Canto Classics. Cambridge: Cambridge University Press (ISBN 978-1-107-60463-6/pbk). 2012, 153p.

[19] O. A. Ivanov, G. M. Fridman, *Discrete Mathematics and Programming in* `Wolfram Mathematica`, Piter Publishers: St Petersburg, 2019, 349p. (in Russian).

[20] A. Jaffe, F. Quinn, *Theoretical mathematics: toward a cultural synthesis of mathematics and theoretical physics*, Bull. Amer. Math. Soc. (N.S.), **29** (1993), no. 1, pp. 1–13; doi: 10.1090/S0273-0979-1993-00413-0

[21] V. Jungić, A. Burazin, *On experimental mathematics and mathematics education.* Amer. Math. Monthly, **128** (2021), no. 9, 832–844.

[22] F. Klein, *Elementarmathematik vom höheren Standpunkte aus. Erster Band: Arithmetik. Algebra. Analysis.* Berlin: Verlag von Julius Springer, 1933. Nachdruck 1968, 309S.

[23] N. N. Konstantinov, A. L. Semenov, *Productive education in the mathematical school. Chebyshevskiĭ Sbornik*, **22** (2021), no. 1 (77), 413–446 (in Russian).

[24] H. Lebesgue, *La mesure des grandeurs.* Nouveau tirage. Paris: Librairie Scientifique et Technique Albert Blanchard. 1975, 184p.

[25] Yu. Manin, *Mathematics as metaphor.* (Selected Essays, with Foreword by F. Dyson). Providence, RI: American Mathematical Society, 2021.

[10]This text was never officially published in French, but there are Russian and Japanese translations, published in 2002 and 2015, respectively.

[26] Yu. Neretin, *On variants of entrance exams.* Moscow Inst. Electronics and Mathematics, Technical report 1999, 8p. (in Russian); `https://www.mat.univie.ac.at/ neretin/obraz/vstup.pdf`

[27] V. A. Rokhlin, *Teaching mathematics to non-mathematicians*, In V. A. Rokhlin—Memorial. Topology, geometry, and dynamics, 19–32, Contemp. Math., 772, Amer. Math. Soc., [Providence], RI, 2021 (First published in English in *Computer Tools in Education*, (2015), no. 3, 50–60).

[28] P. Taylor, *Teach the Mathematics of mathematicians*, Educ. Sci. **8** (2018), no. 2, 56, 10p. `https://doi.org/10.3390/educsci8020056`

[29] W. P. Thurston, *Mathematical education* Notices Amer. Math. Soc., **37** (1990), 844–850.

[30] N. Vavilov, *Reshaping the metaphor of proof*, *Philos Trans. Roy. Soc. A* **377** (2019), no. 2140, pp. 1–18; doi:10.1098/rsta.2018.0279

[31] N. A. Vavilov, *Computers as novel mathematical reality.* I. *Personal account*, Computer Tools in Education, (2020), no. 2, pp. 5–26, (in Russian); doi:10.32603/2071-2340-2020-2-5–26.

[32] N. A. Vavilov, V. G. Khalin, A. V. Yurkov, `Mathematica` *for a non-mathematitian* Electronic textbook, Moscow Centre Continuous Math. Education: Moscow, 2021, 483p. (in Russian), ISBN 978-5-4439-3584-3.

[33] Wu Hung-Hsi; "Order of operations" and other oddities in school mathematics. 2004, 11p. `https://math.berkeley.edu/~wu/ order5.pdf`

[34] D. Zeilberger, *Theorems for a price: tomorrow's semi-rigorous mathematical culture*, Notices Amer. Math. Soc., (1993), no. 40, pp. 978–981; reprinted in Math. Intelligencer, **16** (1994), no. 4. 11–14.

Vladimir Khalin
Dept. of Economics
St Petersburg State University
St Petersburg, Russia
e-mail: `vhalin@yandex.ru`

Nikolai Vavilov
Dept. of Mathematics and Computer Science
St Petersburg State University
St Petersburg, Russia
e-mail: `nikolai-vavilov@yandex.ru`

Alexander Yurkov
Dept. of Economics
St Petersburg State University
St Petersburg, Russia
e-mail: `ayurkov@gmail.com`

0-1 laws in asymptotic combinatorics and central markov measures for continuous graphs

Anatoly Vershik

The concepts of continuous (continual) graded graphs of a special type are introduced. For such kind of continuous graphs the sets of finite paths are convex finite-dimensional compacts, and the central measures are defined by normalized Lebesgue measures on these compacts. They set co-transition probabilities of the central measures. The main example of such graphs are Gelfand-Cetlin type graphs, and graph of spectra of infinite Hermitian matrices.

The problem of describing central measures on the set of paths of such graphs acquires a new character in comparison with previous works on this topic (Pickrel, Vershik-Olshansky), and reduces to the establishment of surprising 0-1 laws for non-stationary Markov chains, or in another way to problems of coincidence or mismatch of geometric and general boundaries of random walks. There is an amazing internal parallelism between lists of central measures of degenerate type for Hermitian matrices (Wishart measures) and for Young graph (discrete Thoma measures) . Even more surprising is the internal similarity between the standard Gaussian measure (GOA or GUI) on matrices and the Plancherel measure on infinite Young diagrams. This work is in progress and partially carried out in cooperation with F.Petrov.

This work is carried out as part of a project supported by an RNF grant 21-11-00152

Anatoly Vershik
St. Petersburg Department of Steklov Institute of Mathematics,on
St. Petersburg State University,
Institute for Information Transmission Problems
St.Petersburg, Russia
e-mail: avershik@gmail.com

WiseTasks Graphs System

Zaikov D.G. and Pozdniakov S.N.

Abstract. The paper presents a learning resource WiseTasks Graphs, which allows you to create graph tasks from various modules. The possibilities of the presented system for various target groups

- of students studying mathematics and algorithms and creating implementations of system modules are illustrated;
- students who use the resource for research activities related to self-formulation and problem solving;
- teachers who are interested in creating constructive problems in graph theory, as well as monitoring the work of students on them;
- students and schoolchildren studying graph theory

The work was supported by the RFBR grant No. 19-29-14141

Introduction

The Wise Tasks Graphs system is designed to create and solve self-testable graph tasks. A self-testable task is such a task, the verification of the solution of which occurs not through reconciliation with a previously saved answer, but through reconciliation with a set condition. For example, if the task is "build a graph that is complete", then in order to understand whether such a problem has been solved correctly, the system needs to check the answer graph for completeness, and not compare it with the complete graphs that are stored in the database of answers.

The main formulation of tasks that can be set within the framework of the system: "Construct a graph with the specified properties...". Another formulation for which the system has verification mechanisms is "specify a subgraph of a given graph that has the properties ...". Other formulations are also allowed, related not only to the allocation of a subgraph, but also to the assignment of various types of marks to its elements, for example, the order of passing edges or vertices of the graph, edge weights, coloring of vertices or edges.

Modules that describe various graph properties and various algorithms on graphs are responsible for various graph properties. By combining different modules, you can create different tasks. This approach allows you to quickly build tasks of a fairly wide class, since to create them you only need to combine different modules. This possibility is provided by the user interface of the "teacher" (note that the concept of "teacher" is conditional here, since the student or student himself has the opportunity to set tasks himself). To introduce numerical characteristics into the problem, in addition to checking for equality with a given number, you can use more and less relations, for example, "build a graph with more than 5 vertices ...".

1. Task example

Here is an example of a new task:

1. Let's choose the modules that we want to add to the task, namely "full graph" and "number of vertices" (Figure 1).

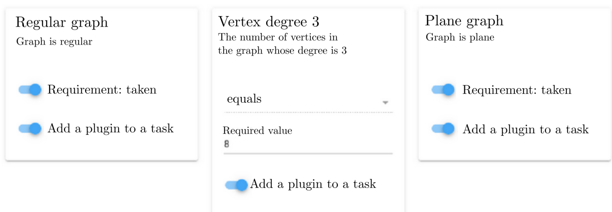


FIGURE 1. Choosing modules

2. Look at the condition that was created according to the selected modules (Figure 2)

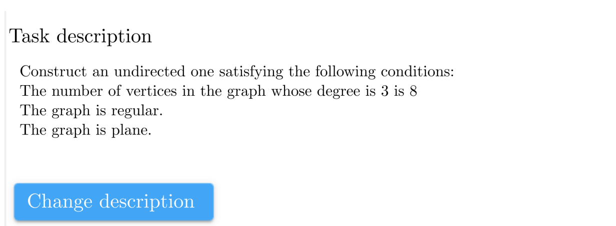


FIGURE 2. Task condition

3. Let's choose the name and category of the task (Figure 3)

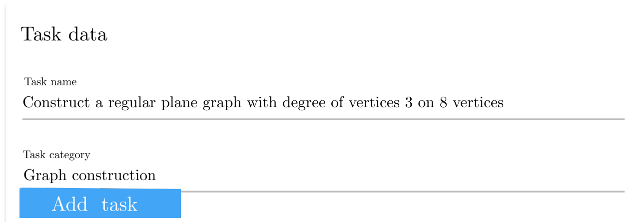


FIGURE 3. Creating task

4. Now let's solve this problem (Figure 4).

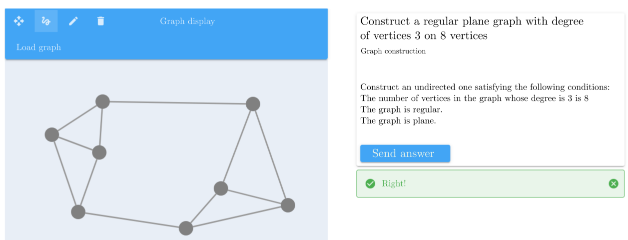


FIGURE 4. Solving task

5. If there are errors in the solution, the system will indicate exactly what the error was (Figure 5)

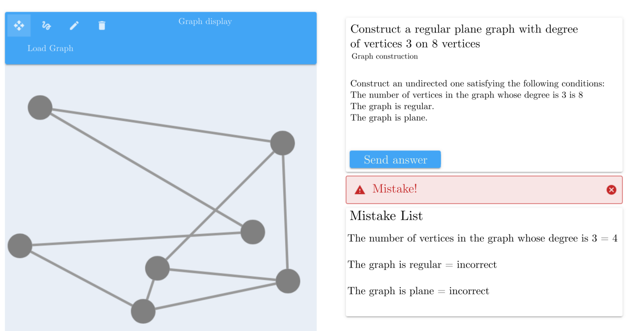


FIGURE 5. Creating mistakes

2. Technical aspects

To work with different types of tasks, the teacher sets the rights for the one who will solve it. In total, there are four types of rights available in the system - adding elements (edges and vertices), setting colors, deleting elements, and setting labels and weights for elements. For each task, you can select a specific set of rights (for example, prohibit deleting and adding elements in a graph, which can be useful in tasks where you want to color an existing graph)

As an example of modules, we will give several properties that are at the same time the names of the modules of the system (Table 1). We distinguish three types of properties: binary properties (whether the graph has the specified properties), numerical characteristics and properties of subgraphs of subgraphs selected in some way.

Binary properties	Numerical characteristics	Marked subgraphs
The constructed graph is a transitive relation graph	Sum of degrees of vertices of an undirected graph	Edges of an undirected graph labeled with natural numbers form an Euler path (traversal in ascending order of labels)
The constructed undirected graph is Euler graph	The clique number ϕ (density) of an undirected graph (the number of vertices in the largest clique)	The marked subset of vertices of an undirected graph is the maximum independent
The constructed undirected graph has a dominant vertex	Vertex connectivity number k (connectivity number) of an undirected graph	The order of traversing the edges of an undirected graph marked by natural numbers is a depth-first traversal (traversal in ascending order of marks)

TABLE 1. Examples of properties

The system assumes three main types of users:

1. A developer is a user who implements new modules in the system, thereby increasing the number of possible tasks to compile
2. A teacher is a user who creates tasks using modules
3. A student is a user who solves these tasks

3. Pedagogical aspects

Since the system is an open web resource, anyone can be a student, a teacher, and a developer, that is, anyone using the web interface can both create modules and participate in filling out the task book by graphs, composing new tasks, and can also solve problems that were compiled by other users.

The “Wise Tasks Graphs” system has already been applied in practice among 2nd year students. 100 tasks were compiled for compiling modules (since the system is written in Java, the modules should have been written in it). The training stream of 100 people was divided into teams, each team had a captain (a person responsible for the correctness of the implementation and testing of modules in the team). Each student was asked to choose and write one module. When writing the module, the student learned to apply the algorithms studied in lectures in practice, which is a good way to consolidate knowledge in the course “Combinatorics and graph theory". Also, writing modules provided students with the opportunity to get acquainted with the Java programming language, which is new for students.

Conclusion

1. The Wise Tasks Graphs system provides verification of graph theory tasks without entering answers to the assigned tasks.
2. The Wise Tasks Graphs system provides conditions for educational and research work on the graph theory course: a student can set and solve problems independently.
3. The Wise Tasks Graphs system allows distributed filling not only with tasks, but also with tool modules describing graph properties and algorithms on graphs.
4. The main problem in filling the Wise Tasks Graphs system is the addition of new modules, since errors in the implemented algorithms will lead to incorrect reactions of the system to the tasks compiled in it. At the same time, the addition of new modules is carried out much less frequently than the addition of new tasks, so ensuring the correct operation of the system requires only the support of the module system, but not the task system.
5. The development of systems like Wise Tasks Graphs allows the organization of new forms of project work of students. So, in the process of filling the system with modules, the distributed work of second-year students of ’LETI’ was organized, who studied the graph theory course and added graph algorithm implementations written in Java to the system.

References

[1] V.A. Emelichev, O.I. Melnikov, V.I. Sarvanov, R.I. Tyshkevich - *Lectures on graph theory*: Nauka Gl. ed. physical and Mathematical lit.

[2] A. A. Voronenko, V. S. Fedorova. *Discrete mathematics. Tasks and exercises with solutions*: An educational and methodical manual.

[3] Pozdniakov S.N., Tolkacheva E.A., Zaikov D.G., Chukhnov A.S. - *Productive learning technologies in creating and using Wise Tasks type resources*

Zaikov D.G.
Saint Petersburg Electrotechnical University 'LETI'
St. Petersburg, Russia
e-mail: dima38091@gmail.com

Pozdniakov S.N.
Saint Petersburg Electrotechnical University 'LETI'
St. Petersburg, Russia
e-mail: pozdnkov@gmail.com

Change and Solve

Eugene V. Zima

Abstract. The change of representation often gives a key to the efficient solution of problems in both numeric and symbolic computation, or in the mixed symbolic-numeric framework.
Popular examples of this technique include but not limited to

- change of basis in polynomial computations,
- modular and evaluation homomorphisms (involving Chinese remaindering or evaluation and interpolation),
- integral representation for computing combinatorial sums,
- fast Fourier transform,
- implicitization of a problem, etc.

In this talk we will give a survey of several popular problems along with discussion of how and why the change of representation improves the theoretical and practical running-time complexity of the employed algorithms. We will consider problems related to the symbolic summation, high-precision evaluation of rapidly convergent series, evaluation of closed form expressions over the regular intervals, and discuss various approaches to their acceleration based on the change of representation [1] - [24].

Discussion will be accompanied by demonstration of software implementations in Maple, Java and C programming languages.

References

[1] S. A. Abramov, M. Petkovšek. D'Alembertian solutions of linear differential and difference equations. In *Proc. of the international symposium on Symbolic and algebraic computation*, 169-174, New York, NY, USA, 1994. ACM Press.

[2] Abramov S.A., Zima E.V. D'alembertian solutions of inhomogeneous linear equations (differential, difference, and some other). In *Proc. of the 1996 International Symposium on Symbolic and Algebraic Computation*, 232-240, New York, NY, USA, 1996. ACM Press.

[3] Abramov S.A., Zima E.V. Minimal completely factorable annihilators. In *Proc. of the 1997 international symposium on Symbolic and algebraic computation*, 290-297, New York, NY, USA, 1997. ACM Press.

[4] S. A. Abramov, M. Petkovšek. Rational normal forms and minimal decompositions of hypergeometric terms. *Journal of Symbolic Computation*, 33(5):521–543, 2002.

[5] Bachmann O., Wang P.S., Zima E.V. Chains of recurrences - a method to expedite the evaluation of closed-form functions. In *Proc. of the international symposium on Symbolic and algebraic computation*, 242-249, New York, NY, USA, 1994. ACM Press.

[6] Bostan A., Chyzak F., Salvy B., Cluzeau T. Low complexity algorithms for linear recurrences. In *Proc. of the 2006 International Symposium on Symbolic and Algebraic Computation*, ISSAC '06, pages 31–38, New York, NY, USA, 2006. ACM.

[7] Cheng H., Zima E.V. On accelerated methods to evaluate sums of products of rational numbers. In *Proc. of the 2000 International Symposium on Symbolic and Algebraic Computation*, 54-61, New York, NY, USA, 2000. ACM Press.

[8] Cheng H., Hanrot G., Thome E., Zima E., Zimmermann P. Time and Space-Efficient Evaluation of Some Hypergeometric Constants, In *Proc. of the International Symposium on Symbolic and Algebraic Computations, ISSAC'2007*, ACM Press, pp. 85-91.

[9] Egorychev G.P., Zima E.V. Integral representation and algorithms for closed form summation. Handbook of Algebra, vol. 5, (ed. M.Hazewinkel), Elsevier, 2008, pp. 459 -529.

[10] Gerhard J., Giesbrecht M, Storjohann A, Zima E.V. Shiftless decomposition and polynomial-time rational summation. In *Proc. of the 2003 International Symposium on Symbolic and Algebraic Computation*, pages 119–126, New York, 2003. ACM.

[11] R. W. Gosper, Jr. Decision procedure for indefinite hypergeometric summation. *Proc. Nat. Acad. Sci. U.S.A.*, 75(1):40–42, 1978.

[12] Kislenkov V., Mitrofanov V., Zima E.V. Multidimensional chains of recurrences. In *Proc. of the 1998 International Symposium on Symbolic and Algebraic Computation*, 199-206, New York, NY, USA, 1998. ACM Press.

[13] B. Salvy, P. Zimmermann, Gfun: a Maple package for the manipulation of generating and holonomic functions in one variable. ACM Transactions on Mathematical Software, vol. 20, no. 2, pp. 163–177, 1994.

[14] Stewart A.M., Zima E.V. Base-2 Cunningham numbers in modular arithmetic. Program. Comput. Software, 2007, vol. 33, pp.80 -86.

[15] Viazmitinov G.L., Zima E.V. A portable interpreter of multidimensional chains of recurrences. Program. Comput. Software, 23(1):2-7, 1997.

[16] Zima E.V. Automatic construction of systems of recurrence relations. USSR Comput. Math. Math. Phys., 24(11-12):193-197, 1984.

[17] Zima E.V. Recurrent relations technique to vectorize function evaluation in loops. In *Proceedings of the 1994 International Conference on Parallel Computation and Cellular Automata*, 161-168. Academy Verlag, 1994.

[18] Zima E.V. Simplification and optimization transformations of chains of recurrences. In *Proc. of the 1995 International Symposium on Symbolic and Algebraic Computation*, 42-50, New York, NY, USA, 1995. ACM Press.

[19] Zima E.V. On parallel construction of multidimensional chains of recurrences. In *Proceedings of the 1996 International Conference on Parallel Computation and Cellular Automata*, 158-167. Academy Verlag, 1996.

[20] Zima E.V. On computational properties of chains of recurrences. In *Proc. of the 2001 International Symposium on Symbolic and Algebraic Computation*, 345-352, New York, NY, USA, 2001. ACM Press.

[21] Zima E.V. Accelerating indefinite summation: Simple classes of summands. *Mathematics in Computer Science*, 7(4):455–472, 2013.

[22] Zima E.V. Accelerating indefinite hypergeometric summation algorithms. *ACM Commun. Comput. Algebra*, 52, 3 (February 2019), pp. 96–99.

[23] Zima E.V. Factorial polynomials in computer algebra problems related to symbolic summation. In *Proc. of 2019 Polynomial Computer Algebra Conference*, 158-161, Euler International Mathematical Institute, St. Petersburg, Russia.

[24] Zima E.V. On the Structure of Polynomial Solutions of Gosper's Key Equation. In *Proc. of the 4th International Conference on Computer Algebra*, 115-119, Moscow, Russia

Eugene V. Zima
Physics and Computer Science dept.,
Wilfrid Laurier University,
Waterloo, Ontario, Canada
e-mail: ezima@wlu.ca