Mathematical Aspects of Computer and Information Sciences

November 13-15, 2019

Gebze, Turkey

Contents

Program

Introduction

MACIS is a series of biennial conferences focusing on research in mathematical and computational aspects of computing and information science. It is broadly concerned with algorithms, their complexity and their embedding in larger logical systems. At the algorithmic level, there is the rich interplay along the Numerical/Algebraic/Geometric/Topological axes. At the logical level, there are issues of data organization, interpretation and associated tools. These issues often arise in scientific and engineering computation where we need experimental and case studies to validate or enrich the theory. MACIS is interested in outstanding and emerging problems in all these areas.

The 8th iteration of MACIS takes place at Gebze Technical University in Gebze/Istanbul (Turkey) in 13-15 November 2019. Previously MACIS was held in Vienna (2017), Berlin (2015), Nanning (2013), Beijing (2011), Fukuoka (2009), Paris (2007) and Beijing 2006.

Organizing Committee
Zafeirakis Zafeirakopoulos (General Chair), Gebze TU, Gebze, Turkey
Daniel Slamanig (PC Chair), AIT Austrian Institute of Technology, Austria
Elias Tsigaridas (PC Chair), Inria/SU/LIP6, Paris, France

Invited Speakers
Matthias Beck,San Francisco State University (USA)
Georg Fuchsbauer,INRIA/ENS (France)
Agnes Szanto, North Carolina State University (USA)

NOVEMBER 13th, WEDNESDAY

9:00	Opening	
9:30	Dorian Florescu and Matthew England. Improved cross-validation for classifiers that make algorithmic choices to minimise runtime without compromising output correctness	T4
10:00	Luca Carlini, Nihat Ay and Christiane Görgen. A numerical efficiency analysis of a common ancestor condition	T4
10:15	Türkü Özlüm Çelik, Asgar Jamneshan, Guido Montúfar, Bernd Sturmfels, and Lorenzo Venturello. Optimal Transport to a Variety	T4
10:45	Break	
11:00	Agnes Szanto. Symbolic-Numeric Certification of Overdetermined and Singular Polynomial Systems	IS
12:00	Lunch	
13:00	Tulay Ayyildiz Akoglu and Agnes Szanto. Certified Hermite Matrices from Approximate Roots - Univariate Case	T1
13:15	Yosuke Sato, Hiroshi Sekigawa, Ryoya Fukasaku and Katsusuke Nabeshima. On Parametric Border Bases	T1
13:30	Manuel Radons. Generalized Perron Roots and Solvability of the Absolute Value Equation	T1
14:00	Sény Diatta, Guillaume Moroz, and Marc Pouget. Reliable Computation of the Singularities of the Projection in $\mathbb{R}^3$ of a Generic Surface of $\mathbb{R}^4$	T1
14:30	Viviane Ledoux and Guillaume Moroz. Evaluation of Chebyshev polynomials on intervals and application to root finding	T1
14:45	Jakob Ablinger. Proving Two Conjectural Series for $\zeta(7)$ and Discovering more Series for $\zeta(7)$	T1
15:00	Break	
15:30	Ali Kemal Uncu. On a weighted spin of the Lebesgue Identity	T3
16:00	Yasemin Büyükçolak, Didem Gözüpek, and Sibel Özkan. Edge-Critical Equimatchable Bipartite Graphs	T3
16:15	Nour Alnajjarine and Michel Lavrauw. Determining the Rank of Tensors in $\mathbb{F}_q^2 \otimes \mathbb{F}_q^3 \otimes \mathbb{F}_q^3$	T3
16:30	Fatma Nur Esirci and Alp Arslan Bayrakçi. Acceleration of Spatial Correlation Based Hardware Trojan Detection Using Shared Grids Ratio	T2
17:00	Metin Evrim Ulu and Murat Cenk. A Parallel GPU Implementation of SWIFFTX	T2
17:30	Break	
17:45	Haoliang Zhang, Hongbo Xu, Jing Ya, Jinqiao Shi and Tingwen Liu. SFV-CNN: Deep Text Sentiment Classification with Scenario Feature Representation	T4
18:15	Muhammad Zubair Islam, Kashif Mehmood and Hyung Seok Kim. Reinforcement Learning Based Interactive Agent for Personalized Mathematical Skill Enhancement	T4
18:45	Sahin Isik and Kemal Ozkan. Common Vector Approach Based Image Gradients Computation for Edge Detection	T4

NOVEMBER 14th, THURSDAY

9:00	Lama Tarsissi and Laurent Vuillon. Second order balance property on Christoffel words	T3
9:30	Michael Wagner, Ludwig Kampel and Dimitris E. Simos. IPO-Q: A Quantum-inspired Approach to the IPO Strategy used in CA generation	T3
10:00	Taha Sevim, Muhammet Selcuk Guvel and Lale Ozkahya. A Fast Counting Method for 6-motifs with Low Connectivity	T3
10:30	Petter Restadh and Per Alexandersson. LaserTank is NP-complete	T3
10:45	Break	
11:00	Matthias Beck. Quasipolynomials in Discrete Geometry and Combinatorial Commutative Algebra	IS
12:00	Lunch	
13:00	Katsusuke Nabeshima and Shinichi Tajima. Generalized integral dependence relations	T1
13:30	Alexander Levin. Hilbert-type dimension polynomials of intermediate difference-differential field extensions	T1
15:00	Hagia Sofia, Basilica Sistern	
18:00	Boshporus Tour	
20:00	Dinner	

NOVEMBER 15th, FRIDAY

9:00	Mijail Borges-Quintana, M. Angel Borges-Trenard, Edgar Martinez-Moro and Gustavo Torres-Guerrero. Computing an invariant of a linear code	T2
9:30	Sanyam Mehta and Vishal Saraswat. Generalized Secret Sharing Schemes using NμMDS Codes	T2
10:00	Hamdi Murat Yıldırım. Exploiting Linearity of Modular Multiplication	T2
10:30	Ana C. Camargos Couto, Marc Moreno Maza, David J. Jeffrey, David Linder and R Corless. Comprehensive LU factors of polynomial matrices	T1
10:45	Break	
11:00	Georg Fuchbauer	IS
12:00	Lunch	
13:00	Angelos Mantzaflaris. An overview of Geometry plus Simulation Modules	SW
13:15	Antonio Jimenez-Pastor. DD-finite functions implemented in Sage	SW
13:30	Ilias Kotsireas. Maple talk	SW
14:00	Break	
14:15	Victor Y. Pan, Qi Luan, John Svadlenka and Liang Zhao. Sublinear Cost Low Rank Approximation via Subspace Sampling	T1
14:45	Victor Y. Pan. Accurate Low Rank Cross-Approximation of a Matrix at Sublinear Cost	T1
15:15	Rémi Imbach and Victor Y. Pan. New practical advances in polynomial root clustering	T1
15:45	Break	
16:00	Chenqi Mou and Jiahua Lai. On the Chordality of Simple Decomposition in Top-Down Style	T1
16:30	Tudor Jebelean and Isabela Dramnesc. Automatic Synthesis of Merging and Inserting Algorithms on Binary Trees using Multisets in Theorema	T1
17:00	Bo Huang and Wei Niu. Algebraic Analysis of Bifurcations and Chaos for Discrete Dynamical Systems	T1
17:30	Bilal Mokhtari, Kamal Eddine Melkemi, Dominique Michelucci and Sebti Foufou. Optimizing Query Perturbations to Enhance Shape Retrieval	T4
18:00	Kettaf Chahrazed and Yousfate Abderrahmane. Authorship attribution by functional discriminant analysis	T4

Abstracts

Improved Cross-Validation for Classifiers that make Algorithmic Choices to Minimise Runtime without Compromising Output Correctness

13 Nov
9:30

Dorian Florescu and Matthew England
Coventry University, Coventry, UK

Our topic is the use of machine learning to improve software by making choices which do not compromise the correctness of the output, but do affect the time taken to produce such output. We are particularly concerned with computer algebra systems (CASs), and in particular, our experiments are for selecting the variable ordering to use when performing a cylindrical algebraic decomposition of n-dimensional real space with respect to the signs of a set of polynomials. In our prior work we explored the different ML models that could be used, and how to identify suitable features of the input polynomials. In the present paper we both repeat our prior experiments on problems which have more variables (and thus exponentially more possible orderings), and examine the metric which our ML classifiers targets. The natural metric is computational runtime, with classifiers trained to pick the ordering which minimises this. However, this leads to the situation were models do not distinguish between any of the non-optimal orderings, whose runtimes may still vary dramatically. In this paper we investigate a modification to the cross-validation algorithms of the classifiers so that they do distinguish these cases, leading to improved results.

A Numerical Effciency Analysis of a Common Ancestor Condition

13 Nov
10:00

Luca Carlini[1,2], Nihat Ay[1], and Christiane Görgen[1]
[1]Max Planck Institute for Mathematics in the Sciences, Leipzig, Germany
[2]Universitá degli Studi di Genova, Italy

The aim of this paper is to understand if the sufficient condition for a common ancestor for some variables in a larger graph discovered by Steudel and Ay is worth checking. The goodness of this criterion will be tested with a numerical method.

---

13 Nov
10:15

Optimal Transport to a Variety

Türkü Özlüm Çelik[1], Asgar Jamneshan[3], Guido Montúfar[1,3], Bernd Sturmfels[1,2], and Lorenzo Venturello[1]

[1]Max Planck Institute for Mathematics in the Sciences, Leipzig, Germany
[2]University of California at Berkeley
[3] University of California at Los Angeles

We study the problem of minimizing the Wasserstein distance between a probability distribution and an algebraic variety. We consider the setting of finite state spaces and describe the solution depending on the choice of the ground metric and the given distribution. The Wasserstein distance between the distribution and the variety is the minimum of a linear functional over a union of transportation polytopes. We obtain a description in terms of the solutions of a finite number of systems of polynomial equations. The case analysis is based on the ground metric. A detailed analysis is given for the two bit independence model.

---

13 Nov
11:00

Symbolic-Numeric Certification of Overdetermined and Singular Polynomial Systems

Agnes Szanto

North Carolina State University, Raleigh, NC, USA

The talk is concerned with certifying that a given point is near an exact root of an overdetermined or singular polynomial system with rational coefficients. The difficulty lies in the fact that consistency of overdetermined systems is not a continuous property. Our certification is based on hybrid symbolic-numeric methods. This is a joint work with Tulay Ayyildiz Akoglu, Jonathan Hauenstein, Bernard Mourrain.

---

13 Nov
13:00

Certified Hermite Matrices from Approximate Roots - Univariate Case

Tulay Ayyildiz Akoglu[1] and Agnes Szanto[2]

[1] Karadeniz Technical University, Trabzon, Turkey
[2]North Carolina State University, Raleigh, NC, USA

Let $f_1, \ldots, f_m$ be univariate polynomials with rational coefficients and $\mathcal{I} := \langle f_1, \ldots, f_m \rangle \subset \mathbb{Q}[x]$ be the ideal they generate. Assume that we are given approximations $\{z_1, \ldots, z_k\} \subset \mathbb{Q}[i]$ for the common roots $\{\xi_1, \ldots, \xi_k\} = V(\mathcal{I}) \subseteq \mathbb{C}$. In this study, we describe a symbolic-numeric algorithm to construct a rational matrix, called *Hermite matrix*, from the approximate roots $\{z_1, \ldots, z_k\}$ and certify that this matrix is the true Hermite matrix corresponding to the roots $V(I)$. Applications of Hermite matrices include counting and locating real roots of the polynomials and certifying their existence.

On Parametric Border Bases

13 Nov
13:15

Yosuke Sato[1], Hiroshi Sekigawa[1], Ryoya Fukasaku[2], and Katsusuke Nabeshima[3]

[1] Tokyo University of Science,Japan
[2] Kyushu University, Japan
[3] Tokushima University, Japan

We study several properties of border bases of parametric polynomial ideals and introduce a notion of a minimal parametric border basis. It is especially important for improving the quantifier elimination algorithm based on the computation of comprehensive Gröbner systems.

Generalized Perron Roots and Solvability of the Absolute Value Equation

13 Nov
13:30

Manuel Radons

Technical University of Berlin

Let A be a real $(n \times n)$-matrix. The piecewise linear equation system $z - A|z| = b$ is called an absolute value equation (AVE). It is well known to be uniquely solvable for all $b \in \mathbb{R}^n$ if and only if a quantity called the sign-real spectral radius of A is smaller than one. We construct a similar quantity that we dub the aligning spectral radius ρ^a of A. Our first main result is that the AVE is solvable for all $b \in \mathbb{R}^n$ if the aligning spectral radius of A is smaller than one. For $n \leq 2$ the AVE is solvable if and only if $\rho^a(A) < 1$. We conjecture that this is also the case for $n > 2$. As our second main result, we devise an algorithm for homotopy solution tracking of the AVE and prove its finite convergence for uniquely solvable systems.

Reliable Computation of the Singularities of the Projection in $\mathbb{R}^3$ of a Generic Surface of $\mathbb{R}^4$

13 Nov
14:00

Sény Diatta[1], Guillaume Moroz[2,3], and Marc Pouget[2,3]

[1]University Assane Seck of Ziguinchor, Sénégal
[2]INRIA, France
[3]LORIA laboratory, Nancy, France

Computing efficiently the singularities of surfaces embedded in $\mathbb{R}^3$ is a difficult problem, and most state-of-the-art approaches only handle the case of surfaces defined by polynomial equations. Let F and G be C^∞ functions from $\mathbb{R}^4$ to $\mathbb{R}$ and $\mathcal{M} = \{(x, y, z, t) \in \mathbb{R}^4 | F(x, y, z, t) = G(x, y, z, t) = 0\}$ be the surface they define. Generically, the surface $\mathcal{M}$ is smooth and its projection Ω in $\mathbb{R}^3$ is singular. After describing the types of singularities that appear generically in Ω, we design a numerically well-posed system that encodes them. This can be used to return a set of boxes that enclose the singularities of Ω as tightly as required. As opposed to state-of-the art approaches, our approach is not restricted to polynomial mapping, and can handle trigonometric or exponential functions for example.

---

13 Nov
14:30

Evaluation of Chebyshev polynomials on intervals and application to root finding

Viviane Ledoux[1,2] and Guillaume Moroz[1]

[1]INRIA, France
[2]École Normale Supérieure

In approximation theory, it is standard to approximate functions by polynomials expressed in the Chebyshev basis. Evaluating a polynomial f of degree n given in the Chebyshev basis can be done in $O(n)$ arithmetic operations using the Clenshaw algorithm. Unfortunately, the evaluation of f on an interval I using the Clenshaw algorithm with interval arithmetic returns an interval of width exponential in n. We describe a variant of the Clenshaw algorithm based on ball arithmetic that returns an interval of width quadratic in n for interval of small enough width. As an application, our variant of the Clenshaw algorithm can be used to design an efficient root finding algorithm.

---

13 Nov
14:45

Proving Two Conjectural Series for $\zeta(7)$ and Discovering more Series for $\zeta(7)$

Jakob Ablinger

Research Institute for Symbolic Computation, Johannes Kepler University, Linz, Austria

We give a proof of two identities involving binomial sums at infinity conjectured by Z-W Sun. In order to prove these identities, we use a recently presented method i.e., we view the series as specializations of generating series and derive integral representations. Using substitutions, we express these integral representations in terms of cyclotomic harmonic polylogarithms. Finally, by applying known relations among the cyclotomic harmonic polylogarithms, we derive the results. These methods are implemented in the computer algebra package `HarmonicSums`.

---

13 Nov
15:30

On a Weighted Spin of the Lebesgue Identity

Ali Kemal Uncu

Austrian Academy of Sciences, Johann Radon Institute for Computational and Applied Mathematics, Linz, Austria

Alladi studied partition theoretic implications of a two variable generalization of the Lebesgue identity. In this short note, we focus on a slight variation of the basic hypergeometric sum that Alladi studied. We present two new partition identities involving weights.

Edge-Critical Equimatchable Bipartite Graphs

13 Nov
16:00

Yasemin Büyükçolak, Didem Gözüpek, and Sibel Özkan
Gebze Technical University, Turkey

A graph is called equimatchable if all of its maximal matchings have the same size. Lesk et al. [5] provided a characterization of equimatchable bipartite graphs. However; it does not explicitly describe the class of equimatchable bipartite graphs. Frendrup et al. [3] also provided a characterization for equimatchable graphs with girth at least five; i.e., a characterization for equimatchable bipartite graphs with girth at least six. In this work, we investigate the structure of a significant subclass of equimatchable bipartite graphs; namely, edge-critical equimatchable bipartite graphs.

References:

3. Frendrup, A., Hartnell, B., Preben, D.; A note on equimatchable graphs. Australasian Journal of Combinatorics 46, 185–190 (2010)
5. Lesk, M., Plummer, M. D.; Pulleyblank, W. R. : Equi-matchable graphs. In: Graph Theory and Combinatorics (Cambridge, 1983), pp. 239–254, Academic Press, London (1984)

Determining the Rank of Tensors in $\mathbb{F}_q^2 \otimes \mathbb{F}_q^3 \otimes \mathbb{F}_q^3$

13 Nov
16:15

Nour Alnajjarine and Michel Lavrauw
Sabanci University, Istanbul, Turkey

Let $\mathbb{F}_q$ be a finite field of order q. This paper uses the classification in [7] of orbits of tensors in $\mathbb{F}_q^2 \otimes \mathbb{F}_q^3 \otimes \mathbb{F}_q^3$ to define two algorithms that take an arbitrary tensor in $\mathbb{F}_q^2 \otimes \mathbb{F}_q^3 \otimes \mathbb{F}_q^3$, and return its orbit, a representative of its orbit, and its rank.

Acceleration of Spatial Correlation Based Hardware Trojan Detection Using Shared Grids Ratio

13 Nov
16:30

Fatma Nur Esirci and Alp Arslan Bayrakci
Gebze Technical University, Turkey

Due to mostly economic reasons almost all countries including the developed ones have to handle integrated circuit designs to a foreign fab for manufacturing, which raises the security issues like intentional malicious circuit (hardware Trojan) insertion by an adversary. A previously proposed method to address these security issues detects hardware Trojan using the spatial correlations in accordance with delay based side channel analysis. However, it is never applied to full circuits and it requires too many path delay computations to select correlated path pairs. In this paper, we first apply the method and present the results for full circuits and then, the method is accelerated by proposing a novel path selection criterion which avoids the computation of path delays. In terms of detection success, the resultant method performs similar to the previous one, but in a much faster fashion.

---

13 Nov
17:00

A Parallel GPU Implementation of SWIFFTX

Metin Evrim Ulu and Murat Cenk
Middle East Technical University, Ankara, Turkey

The SWIFFTX algorithm is one of the candidates of SHA–3 Hash Competition that uses the number theoretic transform (NTT). It has 256–byte input blocks and 65–byte output blocks. In this paper, a parallel implementation of the algorithm and particular techniques to make it faster on GPU are proposed. We target version 6.1 of NVIDIA CUDA compute architecture that employs an ISA (Instruction Set Architecture) called Parallel Thread Execution (PTX) which possesses special instrinsics, hence we modify the reference implementation for better results. Experimental results indicate almost 10x improvement in speed and 5 Watts decrease in power consumption per 2^{16} hashes.

---

13 Nov
17:45

SFV-CNN: Deep Text Sentiment Classification with Scenario Feature Representation

Haoliang Zhang[1,3], Hongbo Xu[1], Jinqiao Shi[2], Tingwen Liu[1] and Jing Ya[1]
[1]Institute of Information Engineering CAS, Beijing, China [2] Beijing University of Posts and Telecommunications, China [3] School of Cyber Security, University of Chinese Academy of Sciences

In this paper, we present a deep learning approach to represent the scenario-related features of a sentence for text classification, and also demonstrate an interesting application which shows the nearest scenarios for a sentence. In order to improve the performance of text classification, it is necessary to make them be aware of the scenario switching at the background of the texts. We propose a CNN based sentiment analysis model named SFV-CNN for sentence classification. The proposed model can be improved by assigning suitable window for each scenario corpus in scenario word embedding training. Our experiments demonstrate that SFV-CNN brings an improvement in accuracy and also shows more obvious advantages when test on datasets across scenarios.

---

13 Nov
18:15

Reinforcement Learning Based Interactive Agent for Personalized Mathematical Skill Enhancement

Muhammad Zubair Islam, Kashif Mehmood, and Hyung Seok Kim
Sejong University, Seoul, Republic of Korea

Traditional Intelligent systems recommend teaching sequence to individual students without monitoring their ongoing learning attitude. It causes frustrations for students to learn a new skill and move them away from their target learning goal. As a step to make the best teaching strategy, in this paper a Personalized Skill-Based Math Recommender (PSBMR) framework has been proposed to automatically recommend pedagogical instructions based on learning literacy progress of a student. PSBMR utilizes an adversarial bandit in contrast to classic multi-armed bandit (MAB) problem to estimate the student's ability and recommend the task as per his skill level. However, this paper proposes an online learning approach to model a student concept learning profile and used Exp3 algorithm for optimal task selection. To verify the framework, simulated students with different behavioral complexity have been modeled using the Q-matrix approach based on item response theory. The simulation study demonstrates the effectiveness of this framework to overcome students negative attitude to acquire the necessary skills to learn basic mathematics.

Common Vector Approach Based Image Gradients Computation for Edge Detection

13 Nov 18:45

Sahin Isik and Kemal Ozkan
Eskisehir Osmangazi University, Eskisehir, TURKEY

In this study, the concept of Common Vector Approach (CVA) is adopted for image gradients computation in terms of revealing edge maps stated on images. Firstly, noise stated on image is smoothed by Gaussian filtering, secondly gradient map computation using CVA is carried out, then the angle and direction maps are obtained from the gradient map and lastly peak points are selected and a smart routing procedure is performed to linking them. With an unusual methodology, the derivatives of image through vertical and horizontal directions have obtained by utilizing the CVA, which is the crucial step and gained the novelty to this work. To compare results objectively, we have judged the performance with respect to a comparison metric called ROC Curve analysis. As a contribution to the edge detection area, CVA-ED presents satisfactory results and edge maps produced can be used in the tasks of object tracking, motion estimation and image retrieval.

Second order balance property on Christoffel words

14 Nov 9:00

Lama Tarsissi[1] and Laurent Vuillon[2]
[1]Univ Gustave Eiffel, UPEM, Univ Paris Est Creteil, France
[2]Univ. Grenoble Alpes, Univ. Savoie Mont Blanc, Chambery, France

We study the *balance matrix* that gives the order of balance of any binary word. In addition, we define for Christoffel words a new matrix called *Second order balance matrix*. This matrix gives more information on the balance property of a word that codes the number of occurrences of the letter 1 in successive blocks of the same length for the studied Christoffel word. By taking the maximum of the Second order balance matrix we define the second order of balance and we are able to give an ordering on Christoffel words. Our construction uses extensively the continued fraction and we prove a recursive formula based on fine properties of the Stern–Brocot tree to construct second order matrices.

IPO-Q: A Quantum-inspired Approach to the IPO Strategy used in CA generation

14 Nov 9:30

Michael Wagner, Ludwig Kampel, and Dimitris E. Simos
SBA Research, Vienna, Austria

Covering arrays are combinatorial structures, that can be considered generalizations of orthogonal arrays and find application in the field of automated software testing amongst others. The construction of covering arrays is a highly researched topic, as previous works relied on heuristic, metaheuristic and combinatorial algorithms to successfully construct covering arrays with a small number of rows. In this paper, we introduce the IPO-Q algorithm which combines a recently introduced quantum-inspired evolutionary algorithm with the widely used in-parameter order (IPO) strategy for covering array generation. We implemented different versions of this algorithm and evaluate them, by means of selected covering array instances, against each other and against an algorithm implementing the IPO strategy.

---

14 Nov
10:00

A Fast Counting Method for 6-motifs with Low Connectivity

Taha Sevim, Muhammet Selçuk Güvel, Lale Özkaya
Hacettepe University, Ankara, Turkey

A k-motif (or graphlet) is a subgraph on k nodes in a graph or network. Counting of motifs in complex networks has been a well-studied problem in network analysis of various real-word graphs arising from the study of social networks and bioinformatics. In particular, the triangle counting problem has received much attention due to its significance in understanding the behavior of social networks. Similarly, subgraphs with more than 3 nodes have received much attention recently. While there have been successful methods developed on this problem, most of the existing algorithms are not scalable to large networks with millions of nodes and edges. The main contribution of this paper is a preliminary study that genaralizes the exact counting algorithm provided by Pinar, Seshadhri and Vishal to a collection of 6-motifs. This method uses the counts of motifs with smaller size to obtain the counts of 6- motifs with low connecivity, that is, containing a cut-vertex or a cut-edge. Therefore, it circumvents the combinatorial explosion that naturally arises when counting subgraphs in large networks. We perform experiments to analyze the motif structure in realworld graphs. To the best of our knowledge, this is the only study that counts 6-motifs using exact computation and performs all counts in graphs with millions of edges in minutes.

---

14 Nov
10:30

LaserTank is NP-complete

Per Alexandersson and Petter Restadh
KTH The Royal Insitute of Technology, Stockholm, Sweden

We show that the classical game LaserTank is NP-complete, even when the tank movement is restricted to a single column and the only blocks appearing on the board are mirrors and solid blocks. We show this by reducing 3-SAT instances to LaserTank puzzles.

---

14 Nov
11:00

Quasipolynomials in Discrete Geometry and Combinatorial Commutative Algebra

Matthias Beck
San Francisco State University and Free University Berlin

A quasipolynomial is a function of the form $q(t) = c_d(t)t^d + \ldots + c_1(t)t + c_0(t)$ where $c_0(t), c_1(t), \ldots, c_d(t)$ are periodic functions. The least common period of $c_0(t), c_1(t), \ldots, c_d(t)$ is the period of $q(t)$, and together with the degree d it gives us an idea about the (computational) complexity of q(t). Quasipolynomials occur frequently as counting functions in combinatorial commutative algebra (as Hilbert functions of monomial algebras) and discrete geometry (as Ehrhart functions of rational polytopes). Using joint work with Maryam Farahmand on antimagic graph counting functions as a guiding example, we present an ansatz to computing quasipolynomials that makes use of techniques from both commutative algebra and discrete geometry.

Generalized Integral Dependence Relations

14 Nov
13:00

Katsusuke Nabeshima[1] and Shinichi Tajima[2]

[1] Tokushima University, Tokushima, Japan
[2] Niigata University, Nishi-ku Niigata, Japan

A generalization of integral dependence relations in a ring of convergent power series is studied in the context of symbolic computation. Based on the theory of Grothendieck local duality on residues, an effective algorithm is introduced for computing generalized integral dependence relations. It is shown, with the aid of local cohomology, generalized integral dependence relations in the ring of convergent power series can be computed in a polynomial ring. The key idea of the proposed algorithm is computing the ideal quotients in a polynomial ring. An extension of the proposed method to parametric cases is also discussed.

Hilbert-type Dimension Polynomials of Intermediate Difference-Differential Field Extensions

14 Nov
13:30

Alexander Levin

The Catholic University of America, Washington, DC, USA

Let K be an inversive difference-differential field and L a (not necessarily inversive) finitely generated difference-differential field extension of K. We consider the natural filtration of the extension L/K associated with a finite system η of its difference–differential generators and prove that for any intermediate difference-differential field F, the transcendence degrees of the components of the induced filtration of F are expressed by a certain numerical polynomial $\chi_{K,F,\eta}(t)$. This polynomial is closely connected with the dimension Hilbert-type polynomial of a submodule of the module of Kähler differentials $\Omega_{L^*|K}$ where L^* is the inversive closure of L. We prove some properties of polynomials $\chi_{K,F,\eta}(t)$ and use them for the study of the Krull–type dimension of the extension L/K. In the last part of the paper, we present a generalization of the obtained results to multidimensional filtrations of L/K associated with partitions of the sets of basic derivations and translations.

Computing an Invariant of a Linear Code

15 Nov
9:00

Mijail Borges-Quintana[1], Miguel Á. Borges-Trenard[2], Edgar Martìnez-Moro[3], and Gustavo Torres-Guerrero[1]

[1]University of Oriente, Santiago de Cuba, Cuba
[2]University Antonio Narino, Bogota, Colombia
[3]University of Valladolid, Castilla, Spain.

In this work, we present an efficient algorithm that generates the leader codewords of a linear code in an incremental form. On the other hand, using the set of leader codewords we define a transformation that remains invariant only if the codes are equivalent which is used as a signature for checking the code equivalence problem. An upper bound on the weight of the codewords is imposed on this algorithm in order to get a smallest set that can be also used as a signature for the 'Code Equivalence Problem'.

---

15 Nov
9:30

Generalized Secret Sharing Schemes using N$^\mu$DS Codes

Sanyam Mehta and Vishal Saraswat

Mehta et. al. [17] recently proposed an NMDS code-based secret sharing scheme which has a richer access structure than the traditional (t, n) threshold secret sharing schemes and admits an access structure based on two groups of subsets of sizes, t and $t-1$, of participants, where $n \geq t > 1$ corresponds to the total number of participants. We give a full generalization of their scheme with complete security proofs. We propose an efficient generalized secret sharing scheme based on N$^\mu$MDS codes in which the computational complexity for setup and reconstruction phases is only $O(n^3)$. The scheme admits an access structure based on $\mu + 1$ mutually exclusive sets of groups of participants of sizes, $t, t-1, \ldots, t-\mu$, respectively, where $1 \leq \mu < t$. The parameter t for the access structure is independent of the field size. The proposed scheme is ideal and perfect and has the desirable security features of cheating detection and cheater identification.

Reference:

17. Mehta, S., Saraswat, V., Sen, S.: Secret sharing using near-MDS codes. In: Codes, Cryptology, and Information Security (C2SI 2019). LNCS, vol. 11445, pp. 195-214. Springer (2019)

---

15 Nov
10:00

Exploiting Linearity of Modular Multiplication

Hamdi Murat Yıldırım

Bilkent University, Ankara, Turkey

The XOR $\oplus$ and the addition $\boxplus$ operations have been widely used as building blocks for many cryptographic primitives. These operations and the multiplication $\odot$ operation are successively used in the design of IDEA and the MESH block ciphers. This work presents several interesting algebraic properties of the multiplication operation. By fixing one operand, we obtain vector valued function g_Z on $\mathbb{Z}_2^n$, associated with $\odot$. In this paper we show that the nonlinearity of g_Z remains the same under some transformations of Z and moreover we give an upper bound for the nonlinearity of g_Z when Z is a power of 2. Under weak-key assumptions, we furthermore present a list of new linear relations for 1-round IDEA cipher, some of directly derived and others algorithmically generated using these relations and known ones. We extend the largest linear weak key class for IDEA cipher with size 2^{23} to derive two such classes with sizes 2^{24} and 2^{27}. Under the independent key subblocks (subkeys) and weak-key assumptions we derive many linear relations for IDEA cipher using linear relations for 1-round IDEA cipher.

Comprehensive *LU* Factors of Polynomial Matrices

15 Nov
10:30

A.C. Camargos Couto[1], M. Moreno Maza[2,3], D. Linder[4], D.J. Jeffrey[3], and R. M. Corless[3]

[1]ORCCA, University of Western Ontario, London ON, Canada
[2]Maplesoft, Waterloo, Ontario, Canada

The comprehensive LU decomposition of a parametric matrix consists of a case analysis of the LU factors for each specialization of the parameters. Special cases can be discontinuous with respect to the parameters, the discontinuities being triggered by zero pivots encountered during factorization. For polynomial matrices, we describe an implementation of comprehensive LU decomposition in Maple, using the `RegularChains` package.

Invited Speaker

15 Nov
11:00

Georg Fuchsbauer

An overview of Geometry plus Simulation Modules

15 Nov
13:00

Angelos Mantzaflaris

Inria Sophia Antipolis - Mediterranee, Universite Cote d'Azur, France

We give an overview of the open-source library "G+Smo". G+Smo is a C++ library that brings together mathematical tools for geometric design and numerical simulation. It implements the relatively new paradigm of isogeometric analysis, which suggests the use of a unified framework in the design and analysis pipeline. G+Smo is an object-oriented, cross-platform, fully templated library and follows the generic programming principle, with a focus on both efficiency and ease of use. The library aims at providing access to high quality, open-source software to the community of numerical simulation and beyond.

DD-finite Functions Implemented in Sage

15 Nov
13:15

Antonio Jimènez-Pastor

Johannes Kepler University, Linz, Austria

We present here the Sage package dd functions which provides symbolic features to work with DD-finite functions, a natural extension of the class of holonomic or D-finite functions, on the computer. Closure properties, composition of DD-finite functions and sequence extraction are key features of this package. All these operations reduce the problem to linear algebra computations where classical division-free algorithms are used.

---

15 Nov
14:15

Sublinear Cost Low Rank Approximation via Subspace Sampling

Victor Y. Pan[1,2], Qi Luan[2], John Svadlenka[2], and Liang Zhao[1,2]

[1]Lehman College and the Graduate Center of the City University of New York, Bronx, NY, USA
[1] The Graduate Center of the City University of New York New York, USA

Low Rank Approximation (LRA) of a matrix is a hot research subject, fundamental for Matrix and Tensor Computations and Big Data Mining and Analysis. Computations with LRA can be performed at *sublinear cost*, that is, by using much fewer arithmetic operations and memory cells than an input matrix has entries. Although every sublinear cost algorithm for LRA fails to approximate the worst case inputs, we prove that our sublinear cost variations of a popular subspace sampling algorithm output accurate LRA of a large class of inputs. Namely, they do so with a high probability (*whp*) for a random input matrix that admits its LRA. In other papers we propose and analyze sublinear cost algorithms for other important matrix computations. Our numerical tests are in good accordance with our formal results.

---

15 Nov
14:45

Accurate Low Rank Cross-Approximation of a Matrix at Sublinear Cost

Victor Y. Pan

Lehman College and the Graduate Center of the City University of New York, Bronx, NY, USA

A matrix algorithm performs at *sublinear cost* if it uses much fewer arithmetic operations than the input matrix has entries. Such algorithms are indispensable for Big Data Mining and Analysis, where the input matrices are so immense that one can only access a small fraction of all their entries. Typically, however, such matrices admit their Low Rank Approximation (LRA), which one can access and process at sublinear cost. Can, however, we compute LRA at sublinear cost? Adversary argument shows that no algorithm running at a sublinear cost can output accurate LRA of the worst case input matrices, or even of the matrices of small families of our Appendix A, but for more than a decade Cross-Approximation (C-A) iterations, running at sublinear cost, have routinely been computing accurate LRA. We partly resolve that long-known contradiction by proving that already a single two-stage C-A loop computes a reasonably close LRA of any matrix that admits LRA, that is, has sufficiently low numerical rank, provided that the C-A loop begins at a submatrix that shares its numerical rank with an input matrix. This provision holds with a high probability (whp) for random input, and we obtain LRA readily if it holds at any recursive C-A step.

New Practical Advances in Polynomial Root Clustering

15 Nov
15:15

Rémi Imbach[1] and Victor Y. Pan[2]

[1]Courant Institute of Mathematical Sciences New York University, USA
[2] City University of New York, USA

We report an ongoing work on clustering algorithms for complex roots of a univariate polynomial p of degree d with real or complex coefficients. As in their previous best subdivision algorithms our root- finders are robust even for multiple roots of a polynomial given by a black box for the approximation of its coefficients, and their complexity decreases at least proportionally to the number of roots in a region of interest (ROI) on the complex plane, such as a disc or a square, but we greatly strengthen the main ingredient of the previous algorithms. Namely our new counting test essentially amounts to the evaluation of a polynomial p and its derivative p', which is a major benefit, e.g., for sparse polynomials p. Moreover with evaluation at about $log(d)$ points (versus the previous record of order d) we output correct number of roots in a disc whose contour has no roots of p nearby. Moreover we greatly soften the latter requirement versus the known subdivision algorithms. Our second and less significant contribution concerns subdivision algorithms for polynomials with real coefficients. Our tests demonstrate the power of the proposed algorithms.

On the Chordality of Simple Decomposition in Top-Down Style

15 Nov
16:00

Chenqi Mou[1] and [2]Jiahua Lai

[1]LMIB-School of Mathematical Sciences, Beihang University, Beijing, China
[2]Beijing Advanced Innovation Center for Big Data and Brain Computing, Beihang University, Beijing, China

Simple decomposition of polynomial sets computes conditionally squarefree triangular sets or systems with certain zero or ideal relationships with the polynomial sets. In this paper we study the chordality of polynomial sets occurring in the process of simple decomposition in top-down style. We first reformulate Wang's algorithm for simple decomposition in top-down style so that the decomposition process can be described in an inductive way. Then we prove that for a polynomial set whose associated graph is chordal, all the polynomial sets in the process of Wang's algorithm for computing simple decomposition of this polynomial set have associated graphs as subgraphs of the input chordal graph.

---

15 Nov
16:30

Automatic Synthesis of Merging and Inserting Algorithms on Binary Trees using Multisets in *Theorema*

Isabela Dramnesc[1] and Tudor Jebelean[2]
[1]West University, Timisoara, Romania
[2]Johannes Kepler University, Linz, Austria

We demonstrate the automatic proof-based synthesis of merging and inserting algorithms for [sorted] binary trees, using the notion of multisets, in the *Theorema* system. Each algorithm is extracted from the proof of the conjecture based on the specification of the desired function, in the form of a list of [conditional] equalities, which can be directly executed. The proofs are performed in natural style, using general techniques, but most importantly efficient inference rules and strategies specific for the domains involved. In particular we present specific techniques for the construction of arbitrarily nested recursive algorithms by general Noetherian induction, as well as a systematic method for the generation of the conjectures and consequently of the algorithms for the auxiliary functions needed in the main function.

---

15 Nov
17:00

Algebraic Analysis of Bifurcations and Chaos for Discrete Dynamical Systems

Bo Huang[1,2] and Wei Niu[3,4]
[1]LMIB-School of Mathematics and Systems Science, Beihang University, Beijing, China
[2]Courant Institute of Mathematical Sciences, New York University, New York, USA
[3]Ecole Centrale de Pekin, Beihang University, Beijing, China
[4]Beijing Advanced Innovation Center for Big Data and Brain Computing, Beihang University, Beijing, China

This paper deals with the stability, bifurcations and chaotic behaviors of discrete dynamical systems by using methods of symbolic computation. We explain how to reduce the problems of analyzing the stability, bifurcations and chaos induced by snapback repeller to algebraic problems, and solve them by using an algorithmic approach based on the methods for solving semi-algebraic systems. The feasibility of the symbolic approach is demonstrated by analyses of the dynamical behaviors for several discrete models.

---

15 Nov
17:30

Optimizing Query Perturbations to Enhance Shape Retrieval

Bilal Mokhtari[1], Kamal Eddine Melkemi[2], Dominique Michelucci[3], and Sebti Foufou[4]
[1]Biskra university, Algeria
[2]Batna university, Algeria
[3]Dijon university, France
[4]New York University, Abu Dhabi, United Arab Emirates

3D Shape retrieval algorithms use shape descriptors to identify shapes in a database that are the most similar to a given key shape, called the query. Many shape descriptors are known but none is perfect. Therefore, the common approach in building 3D Shape retrieval tools is to combine several descriptors with some fusion rule. This article proposes an orthogonal approach. The query is improved with a Genetic Algorithm. The latter makes evolve a population of perturbed copies of the query, called clones. The best clone is the closest to its closest shapes in the database, for a given shape descriptor. Experimental

results show that improving the query also improves the precision and completeness of shape retrieval output. This article shows evidence for several shape descriptors. Moreover, the method is simple and massively parallel.

Authorship attribution by functional discriminant analysis

15 Nov
18:00

Chahrazed Kettaf and Abderrahmane Yousfate
Laboratoire de Mathmatiques, DJILLALI LIABES University, SIDI BEL ABBES,Algeria

Recognizing the author of a given text is a very difficult task that relies on several complicated and correlated criterias. For this purpose, several classification methods are used (neuronal network, discriminant analysis, SVM ...). But a good representation of the text that keeps the maximum of the stylistic information is very important and has a considerable influence on the result. In this paper, we will tackle the problem of the authorship attribution for very long texts using the discriminant analysis extended to the functional case after presenting the texts as elements of a separable Hilbert space.

Author Index