siam® 2023

Searchable Abstracts Document

Conference on Applied Algebraic Geometry (AG23)

July 10–14, 2023

This document was current as of June 26, 2023. Abstracts appear as submitted.

siam®
3600 Market Street, 6th Floor
Philadelphia, PA 19104-2688 U.S.
Telephone: 800-447-7426 (U.S. & Canada) +1-215-382-9800 (Worldwide)
meetings@siam.org

IP1
Why We Decompose Tensors

Tensor decomposition, interpreted broadly as expressing a higher-order tensor in terms of numbers, vectors, and other lower-order tensors, is omnipresent in pure and applied mathematics. For example, tensor decomposition and related notions of tensor rank feature in signal processing, algebraic statistics, the cap-set problem, and Stillman's conjecture. This ubiquity is an important answer to the question implicit in the title. However, that question also admits a different type of answer: purely mathematical theorems that explain this omnipresence of tensor decomposition. Roughly speaking, these theorems say that any property of tensors that is preserved under restriction (the application of linear maps to the tensor factors) implies some form of tensor decomposition. For instance, for symmetric tensors, a theorem by Kazhdan-Ziegler says that any restriction-closed property implies a uniform bound on the Schmidt rank. In characteristic zero, the picture has become particularly clear through joint work with Bik-Danelon-Eggermont-Snowden. In positive characteristic, the best theorem is not yet known, but I will report on work with Blatter-Rupniewski on the case of finite fields. Here, in a theorem that bears a striking resemblance to the graph minor theorem, we show that any restriction-closed property of tensors can be characterised by a finite set of forbidden restrictions.

Jan Draisma
Mathematical Institute, University of Bern, Switzerland
jan.draisma@math.unibe.ch

IP2
Hey AI, What's New in Science in 2026?

By some metrics, machines could answer the above question with over 90% accuracy. Why was this problem so "easy"? What was the math behind such a model? What should we, as researchers, do next? Join me for some math, some intuition, and some anecdotes on winning and losing data competitions.

Ngoc Tran
University of Texas at Austin
Department of Mathematics
ntran@math.utexas.edu

IP3
Threshold-linear Networks, Attractors, and Oriented Matroids

Threshold-linear networks (TLNs) are common firing rate models in theoretical neuroscience that are useful for modeling neural activity and computation in the brain. They are simple, recurrently-connected networks with a rich repertoire of nonlinear dynamics including multistability, limit cycles, quasiperiodic attractors, and chaos. Over the past few years, we have developed a mathematical theory relating stable and unstable fixed points of TLNs to combinatorial properties of an underlying graph. The resulting ”graph rules” and ”gluing rules” provide a direct link between network architecture and key features of the dynamics. Many open questions remain, however, such as: How do changes in network parameters, such as connectivity, transition a TLN from one dynamic regime to another? In this talk, I present some new results in the bifurcation theory of TLNs, with an eye towards understanding how these networks may evolve via training (or learning). It turns out that a certain family of determinants related to the underlying hyperplane arrangement of a TLN is key. In particular, the theory of oriented matroids and Grassmann-Plucker relations provide valuable insights into the allowed fixed point configurations of TLNs, as well as the allowed bifurcations.

Carina Curto
Pennsylvania State University
cpc16@psu.edu

IP4
Factorising Data

Data contains algebraic structure, which can be leveraged to understand the systems it describes. We can find structure in data by factorising (or, factoring) it into building blocks, which should be interpretable for the context at hand. In this talk, I will discuss matrix and tensor decompositions that arise when factorising data, and the linear and multilinear algebra that underpins their theoretical properties. We will see examples from applications such as graphical models, time series, and causal disentanglement.

Anna Seigal
Harvard University, U.S.
aseigal@seas.harvard.edu

IP5
Multistationarity and Absolute Concentration Robustness in Biochemical Reaction Networks

Reaction networks arising in systems biology are often modeled with mass-action kinetics. This setup generates systems of polynomial ODEs involving many (typically unknown) parameters. Two important properties that such systems may possess are multistationarity and absolute concentration robustness (ACR). Multistationarity refers to the capacity for two or more steady states (mathematically, this means two or more positive real solutions to a system of polynomials), while ACR pertains to when some species concentration is the same at all positive steady states (that is, a certain positive real variety lies in a hyperplane of the form $x_i = c$). This talk showcases networks arising in applications that have multistationarity or ACR, and describes recent analyses of these properties by algebraic methods (specifically, involving steady-state parametrizations, mixed-volume computations, and real radical ideals). We also highlight new results on the prevalence of multistationarity and ACR in randomly generated reaction networks; in particular, we show that these two properties rarely occur together (mirroring what is seen in applications). The results in this talk come from several joint works with many co-authors: C. Conradi, L. Garcia Puente, E. Gross, H. Harrington, M. Johnston, B. Joshi, N. Kaihnsa, N. Meshkat, T. Nguyen, N. Obatake, M. Perez Millan, X. Tang, and A. Torres.

Anne Shiu
Texas A&M University, U.S.
annejls@math.tamu.edu

IP6
Localization and Mapping from Images

Image-based localization and mapping are a crucial tasks for a wide range of applications, from augmented reality to self-driving cars. In this talk, I will give an overview of sparse 3D reconstruction pipelines, focusing on the challenges of dealing with outlier contaminated data. To address these challenges, robust estimation methods are necessary and the current paradigm is to rely on hypothesize-and-test frameworks that require estimating models from as few measurements as possible. These estimation problems, known as minimal problems, can generally be formulated as solving a set of polynomial equations. I will give an overview of how these problems appear and the solution strategies that are employed in practice. I will also highlight the connections with algebraic geometry, discuss the open problems and opportunities for further research.

Viktor Larsson
Lund University, Sweden
viktor.larsson@math.lth.se

IP7

Signal Recovery on an Algebraic Variety from Linear Samples

Signal recovery on an algebraic variety is an essential problem in many applications. Many well-known problems, such as compressed sensing, phase retrieval and low-rank matrix recovery, can be viewed as a signal recovery problem on an algebraic variety. A fundamental question is: How many measurements are needed to recover (almost) all the signals lying on an algebraic variety? In this talk, we focus on the problems of phase retrieval and low-rank matrix recovery. We use the tools from algebraic geometry to study the question and present many results to address it in many different settings. We also introduce the performance of several numerical models for solving these problems.

Zhiqiang Xu
AMSS, Chinese Academy of Sciences
xuzq@lsec.cc.ac.cn

IP8

Maximal Curves Over Finite Fields

Algebraic curves over a finite field $\mathbb{F}_q$ have been a source of great fascination, ever since the seminal work of Hasse and Weil in the 1930s and 1940s. Many fruitful ideas have arisen out of this area, where number theory and algebraic geometry meet. A very famous example was provided in 1977-1982 by Goppa, who found applications to coding theory. The key point of Goppa's construction is that the code parameters are essentially expressed in terms of the features of the curve, such as the number N_q of $\mathbb{F}_q$-rational points and the genus g. Goppa codes with good parameters are constructed from curves with large N_q with respect to their genus g. Given a smooth projective, algebraic curve of genus g over $\mathbb{F}_q$, an upper bound for N_q is a corollary to the celebrated Hasse-Weil Theorem,

$$N_q \leq q + 1 + 2g\sqrt{q}.$$

Curves attaining this bound are called $\mathbb{F}_q$-maximal. The Hermitian curve is a key example of an $\mathbb{F}_q$-maximal curve, as it is the unique curve, up to isomorphism, attaining the maximum possible genus of an $\mathbb{F}_q$-maximal curve. It is a result commonly attributed to Serre that any curve which is $\mathbb{F}_q$-covered by an $\mathbb{F}_q$-maximal curve is still $\mathbb{F}_q$-maximal. In particular, quotient curves of $\mathbb{F}_q$-maximal curves are $\mathbb{F}_q$-maximal. Many examples of $\mathbb{F}_q$-maximal curves have been constructed as quotient curves of the Hermitian curve by choosing a subgroup of its very large automorphism group. It is a challenging problem to construct maximal curves that cannot be obtained in this way, as well as to construct maximal curves with many automorphisms (in order to use the machinery described above). In this talk, we will describe our main contributions to the theory of maximal curves over finite fields and their applications to coding theory. The following topics will be discussed:

1. How to decide whether a maximal curve is a quotient of the Hermitian curve;
2. Maximal curves with many automorphisms;
3. Weierstrass semigroups and codes from maximal curves.

Maria Montanucci
Department of Applied Mathematics and Computer Science
Technical University of Denmark
marimo@dtu.dk

IP9

Sums of Squares of Polynomials for Matrix Copositivity and Stable Sets in Graphs

Sums of squares of polynomials offer a powerful tool for the design of tractable approximations for many hard problems arising in discrete and continuous optimization, combinatorial matrix theory, and more. While there exist nonnegative polynomials that are not sums of squares (Hilbert 1988), for every nonnegative polynomial p there exists a polynomial q such that q^2p is a sum of squares, thus giving a positivity certificate ‘with denominator (Artin 1927). When p is homogeneous and strictly positive the denominator can be chosen to be a power of $\sum_i x_i^2$ (Reznick 1995). Positivity certificates ‘without denominator exist for strictly positive polynomials on compact sets like the unit sphere or the simplex (Schmdgen 1991, Putinar 1993). This lecture revolves around the question of testing matrix copositivity, which can be formulated as testing nonnegativity of a quadratic form (over the nonnegative orthant or the simplex), or of a quartic form (on the full space or the unit sphere). Various positivity certificates lead to various conic approximations of the copositive cone. We discuss old and new results about these conic approximations, their mutual relationships, and when they are sufficient to fully describe copositive matrices. We also discuss their application to finding bounds for stable sets in graphs and finite convergence properties of these bounds. Based on joint work with Felipe Luis Vargas (CWI).

Monique Laurent
Centrum Wiskunde & Informatica (CWI)
Amsterdam, and Tilburg University
M.Laurent@cwi.nl

IP10

Recent Advances in Computational Algebra and Polynomial System Solving Through Grbner Bases

Computational algebra and related geometric problems arise in a number of engineering sciences such as robotics, computer vision or biology. This encompasses the computation of kinematic singularities, the location and characterization of singularities of dynamical systems and their stability analysis, the classification of real roots to systems depending on parameters, or the topological analysis of real solution sets to polynomial systems such as the determination of their number of connected components. The cornerstone of the computational machinery needed to tackle these problems consists in representing and manipulating algebraic sets defined by polynomial equations and inequations. Because they generally do not need any special assumptions on the input, and thanks to the exactness of their output, Grbner bases algorithms are key players in this area however they have not always been designed with a geometric context in mind. Thus, a fundamental issue is to design a new generation of algorithms, more efficient and better suited to geometric problems. In this talk, we will present new algorithms for computing Grbner bases of saturated polynomial ideals and for changing monomial orderings. These are used for computing Zariski closures of set theoretic differences of algebraic sets as well as projections of algebraic sets. This talk will be illustrated by examples coming from applications where the use of symbolic computation is crucial.

Mohab Safey El Din
Sorbonne University, France
Mohab.Safey@lip6.fr

SP1

SIAM Activity Group on Algebraic Geometry Early Career Prize Lecture: Exact Semidefinite Relaxations for Polynomial Optimization and Applications in Euclidean Distance Problems

Polynomial optimization problems are ubiquitous in applications, but they are notoriously difficult to solve. Semidefinite programming (SDP) relaxations provide a tractable way to approximate such hard problems. We will discuss tools that allow to analyze the quality of such relaxations. We are particularly interested in understanding when the relaxation solves the original polynomial optimization problem exactly. A notable class of problems under consideration are Euclidean distance problems, in which the goal is to find the nearest point to a given one in an algebraic variety. These problems arise in several denoising problems from statistics, computer science, and engineering. We show that SDP relaxations often solve them exactly in the low noise regime. We also point out connections between such SDP relaxations and Voronoi cells of varieties.

Diego Cifuentes
Georgia Institute of Technology, U.S.
diego.cifuentes@isye.gatech.edu

CP1

A New Method to Solve the Elliptic Curve Discrete Logarithm Problem

We have developed a new probabilistic algorithm called the Las Vegas algorithm to solve the ECDLP [Ayan, A Las Vegas algorithm to solve the ECDLP, 2018] which was further improved [Abdullah, A new method for solving the ECDLP, 2021] to include the initial minor conjecture. This presentation is in the direction of finding a proper set of minors for the initial minor conjecture. The Las Vegas algorithm produces a $\ell \times 2\ell$ matrix $\mathcal{K}$ which is a basis of an ℓ-dimensional subspace of a 2ℓ dimensional vector space over $\mathbb{F}_q$. This subspace is the left kernel of a well-defined matrix. This attack reduces ECDLP to a problem in linear algebra which we call the zero-minor problem. The problem is: to find a zero minor in a non-singular matrix. As the number of minors is exponential in the size of the matrix, this poses a significant challenge. Thus we propose the initial minor conjecture; which says, it is enough to look at a small set of minors to determine if the matrix has a zero-minor. In this presentation, we show recent progress in solving this problem. Our results are experimental in nature. We show by computer simulation that there are certain sets of minors that show a lot of promise. We have studied many sets of minors, which have polynomial size in ℓ, to solve ECDLP. This shows that we are on the right track to find a set of initial minors. If that set is polynomial in ℓ, we will have a polynomial time algorithm to solve ECDLP

Abdullah Z. Ansari
Savtribai phule pune university
abdullah0096@gmail.com

CP1

Hearing Shapes with P-Adic Laplacians

For a finite combinatorial graph, a spectral curve is constructed as the zero set of a two-variate polynomial with integer coefficients coming from p-adic diffusion on the graph whose diffusion constants are natural numbers. It is shown that certain spectral curves can distinguish non-isomorphic pairs of isospectral graphs, and can even reconstruct the graph by playing a game in which the spectra depending on a chosen prime number can be asked for. It is shown that there is a winning strategy in this game which allows the reconstruction of the graph from the spectra of the associated p-adic Laplacian operators, if the diffusion constants are chosen properly. The reason is that the non-zero coefficients of the polynomial defining the spectral curve then have absolute value one. This implies that the number of certain types of spanning forests controlled by these diffusion constants is either one or zero, and the uniqueness of the combinatorial graph follows. As an application to p-adic geometry, it is shown that playing this game allows to recover the reduction graph of a Mumford curve and the product reduction graph of a p-adic analytic torus from the spectrum of such operators.

Patrick E. Bradley, Angel Ledezma
Karlsruhe Institute of Technology
Institute of Photogrammetry and Remote Sensing
bradley@kit.edu, angel.ledezma@kit.edu

CP1

New Approach Based on Algebra Tools for Set-membership Detectability in Case of Multiple Faults

The first part of a fault-diagnosis approach consists in verifying the detectability property which is the capacity to detect the occurrence of faults in the system. But complex systems are subjected to uncertainties making the modeling task awkward. It is particularly difficult to get an accurate model of the perturbations and noises acting on the system. This may turn the usual stochastic framework and this is why stochastic models are sometimes disregarded to the benefit of set-membership models. These naturally cope with uncertain and inaccurate knowledge when perturbations and noises are assumed to be bounded but otherwise unknown. This work presents an original approach for assessing multiple fault detectability of nonlinear parametrized dynamical models, with bounded uncertainties. A future extension of this work consists in considering measurement noise modeled by probability density functions. The proposed method is based on computer algebra algorithms, such as the RosenfeldGroebner algorithm which permits to eliminate the unknown variables of the model. Thus some precomputed values of algebraic expressions characterizing the presence of faults are returned.

Estimations of these expressions, obtained from input and output measurements, permit then the detection and isolation of multiple faults acting on the system. This approach is applied on a coupled water-tank model and highlights the potential of the suggested approach.

Carine Jauberthie
LAAS-CNRS
carine.jauberthie@laas.fr

Nathalie Verdière
Le Havre University
nathalie.verdiere@univ-lehavre.fr

CP1

Bounds on Embeddings of Triangulations of Spheres

Borcea and Streinu showed that the upper bound of the number of congruence classes of a minimally d-volume rigid $(d+1)$-uniform hypergraph on n vertices in $\mathbb{R}^d$ increases exponentially in n and d. We show that this result also holds for triangulations of $\mathbb{S}^2$ in $\mathbb{R}^2$, and then find a geometrically motivated bound linear in n for bipyramids. By the methods used to deduce this bound, we show that, in general, global d-volume rigidity in $\mathbb{R}^d$ is not a generic property of a $(d+1)$-uniform hypergraph.

Jack Southgate
University of St Andrews
jos3@st-andrews.ac.uk

CP2

Implicitization of A Plane Curve Germ

Let Y = f(x, y) = 0 be the germ of an irreducible plane curve. We present an algorithm to obtain polynomials, whose valuations coincide with the semigroup generators of Y. These polynomials are obtained sequentially, adding terms to the previous one in an appropriate way. To construct this algorithm, we perform truncations of the parametrization of Y induced by the Puiseux Theorem. Then, an implicitization theorem of Tropical Geometry for plane curves is applied to the truncations. The identification between the local ring and the semigroup of Y plays a key role in the construction of the algorithm, allowing us to carry out a formal elimination process, which we prove to be finite. The complexity of this elimination process equals the complexity of a integer linear programming problem. This algorithm also allows us to obtain an approximation of the series f, with the same multiplicity and characteristic exponents. We present a pseudocode of the algorithm and examples, where we compare computation times between an implementation of our algorithm and elimination through Grbner bases.

Ana Casimiro, João Cabral
Universidade Nova de Lisboa
amc@fct.unl.pt, jpbc@fct.unl.pt

CP2

Effective Birational Deformation of Trilinear Volumes

We present effective methods to manipulate birational tensor-product maps $\phi : (\mathbb{P}^1_{\mathbb{C}})^3 \dashrightarrow \mathbb{P}^3_{\mathbb{C}}$ defined by four trilinear polynomials f_0, f_1, f_2, f_3, which are the first for the construction of non-affine birational maps in 3D. Namely, we describe all the possible minimal graded free resolutions of the ideal $I = (f_0, f_1, f_2, f_3)$ and provide the complete list of isomorphism classes of the base loci defined by I [Bus L., Gonzlez-Mazn, P., Schicho, J., Tri-linear birational maps in dimension three, Mathematics of Computation]. Based on these results, we give formulas for the efficient computation of weights for the Bzier control points of ϕ that yield birationality, and compute the inverse rational map explicitly [Gonzlez-Mazn, P., Bus L., Birational 3D free-form deformations of degree $1 \times 1 \times 1$, Preprint]. According to the degree of the inverse ϕ^{-1}, we find different classes of birational maps. The first is the class of hexahedral maps, i.e. the control points determine a quadrilaterally-faced hexahedron. Hexahedral birational maps are the direct generalization to 3D of 2D quadrilateral birational maps [Sederberg T.W., Zheng J., Birational quadrilateral maps, Computer Aided Geometric Design]. In the remaining classes, the inverse rational map is quadratic for one of the parameters and the geometry of the control points is related to doubly ruled quadric surfaces.

Pablo González-Mazón
Centre INRIA d'Université Côte d'Azur
pablo.gonzalez-mazon@inria.fr

CP2

Numerical Computation of the Homology and Periods of Complex Surfaces

The period matrix of a smooth complex projective algebraic variety encodes the duality between singular homology and DeRham cohomology given by the DeRham theorem. Its entries, called periods, are integrals of algebraic forms on homological cycles. This matrix carries information about fine algebraic invariants of the variety (as shown by Torelli-type theorems, for instance), and periods also arise in theoretical physics (Feynman integrals). We provide a direct method to efficiently compute numerical approximations of the period matrix of a complete intersection. More precisely, our method relies on an effective Picard-Lefschetz theory, from which we obtain an explicit description of the cycles that is well suited for numerical integration. This allows us to compute the holomorphic periods of generic quartic surfaces, which encodes the Hodge decomposition of the variety. This computation can be done an hour, which was previously unattainable. In this lecture, I will give a description of this method. This is joint work with my advisors P. Lairez and P. Vanhove.

Eric Pichon-Pharabod
Université Paris-Sud
eric.pichon@polytechnique.edu

Pierre Lairez
Inria Saclay le-de-France
pierre.lairez@inria.fr

Pierre Vanhove
Institut de Physique Théorique (IPhT) at CEA Saclay, France
pierre.vanhove@ipht.fr

CP3

Nonlinear Algebraic Data Analysis

Analytical methods based on linear algebra are ubiquitous primarily due to their computational feasibility, but real-world data is typically nonlinear. Nonlinear algebra is emerging as a distinct research field from several separate efforts - tensor analysis, numerical linear algebra, mathematical models of (deep) neural networks, and invariant theory. The application of nonlinear algebraic methods to data analysis has the potential to more accurately and faithfully model complex, real-world data. In this talk, I will present how methods from numerical algebraic geometry can be used to represent data as algebraic varieties and how these representations can be used to perform classification, a typical machine learning (ML) task. The performance of this novel Algebraic Variety Classification method will be compared to standard ML algorithms on a number of public datasets, with issues regarding learning varieties from samples and numerical considerations discussed. I will also explore how these methods can be developed into a framework for other common learning tasks such as feature extraction and forecasting.

Jonathan Gryak
Queens College, City University of New York (CUNY)
jgryak@qc.cuny.edu

CP3

Weak Maximum Likelihood Threshold of Coloured Gaussian Graphical Models

Colored graphical models are linear concentration models arising from undirected graphs with a coloring in its vertices and edges. Given a colored Gaussian graphical model, one may be interested to know how many observations are necessary for a maximum likelihood estimate to exist with positive probability. This is called the weak maximum likelihood threshold of a graph. We present novel computational and algebraic methods for studying the weak maximum likelihood threshold of a graph.

Olga Kuznetsova
Aalto University, Department of Computer Science
kuznetsova.olga@gmail.com

Roser Homs Pons
Centre de Recerca Matemàtica, Spain
rhoms@crm.cat

CP3

On the Use of $\mathfrak{sl}_2$-Representations in Feed-Forward Networks

In this paper [Mokhtari & Rink, 2023, preprint], we study the normal forms of feed-forward networks. These types of networks are one of the classes of networks for which the node's connections are loop-free and the cells only have input from the cells below. To study the local behavior of the dynamical systems in the vicinity of a singular point we use normal form theory. The normal form of a given dynamical system is the equivalent form of a system that can be obtained by employing near-identity coordinate transformations. The $\mathfrak{sl}$-style of normal form for vector fields was introduced in [Cushaman & Sanders, 1986]. Assume that the dynamical system $\dot{x} = Nx + f(x)$ with $x \in \mathbb{R}^n$ and nilpotent N is given. The Jacobson-Morozov theorem guarantees the existence of a nilpotent M and a semisimple operator H such that $\langle M, N, H \rangle$ form an $\mathfrak{sl}_2$ triple. Then, the normal form by those elements which are in the $\ker \operatorname{ad}(M)$. However, at first sight, these technical conditions are not met in our feed-forward network. In this talk, we study the normal forms of fully inhomogeneous feed-forward network, with the nilpotent linear part. A new method for classifying the normal form, the triangular $\mathfrak{sl}_2$-style, is introduced. In order to formulate a normal form theory up to quadratic terms, we use Hermite reciprocity, transvectants, and results for the 3-dimensional normal forms.

Fahimeh Mokhtari
Department of mathematics (VU Amsterdam)
f.mokhtari@vu.nl

Bob Rink
Vrije Universiteit Amsterdam
b.w.rink@vu.nl

CP3

Identifiability of Statistical Models with Latent Symmetries

We study a class of graphical models having two layers of vertices, corresponding to latent and observable variables, all edges being directed from the latents to the observables. These and similar models were first studied in the neural networks literature, where they correspond to one level of computation; subsequently, such models have been studied in algebraic statistics. We are interested in the case that the model is invariant under permutation of the latent variables. We show that the parameters of the model are identifiable at the least possible number of observables at which this might be so. The proof relies on a root interlacing phenomenon.

Leonard Schulman
Caltech
schulman@caltech.edu

Spencer Gordon
U Liverpool
slgordon@caltech.edu

CP4

Uniform Density in Matroids, Matrices and Graphs

A matroid M is uniformly dense if $\operatorname{rank}(M|X)/|M|X| \geq \operatorname{rank}(M)/|M|$ for all nonempty restrictions $M|X$. These matroids are extremal for certain connectivity, packing and covering properties and have applications in the design of robust networks [Catlin et al., Fractional arboricity, strength, and principal partitions in graphs and matroids, 1992]. In this talk, I will discuss new characterizations of uniform density derived from the geometry of matroid polytopes. As a first application, we show that uniformly dense real-representable matroids (i.e. real matrices) are parametrized by constant-diagonal projection matrices, which form a real algebraic variety. The proof makes use of the moment map on the Grassmannian and the theory of determinantal probabilities. As a second application, we show that regular uniformly dense graphic matroids are 1-tough: removing any k vertices from the graph results in at most k connected components. This talk is based on joint work with Raffaella Mulas.

Karel Devriendt
Max Planck Institute for Mathematics in the Sciences
karel.devriendt@mis.mpg.de

Raffaella Mulas
Vrije Universiteit Amsterdam

r.mulas@vu.nl

CP4

Positivity for Tropical Flag Varieties

In this talk we will study different positivity notions that exist for tropical flag varieties. These include: the tropicalization of a totally non-negative flag variety, the tropicalization of the intersection of a flag variety with the positive orthant and the space of valuated flag matroids which induce subdivisions into Bruhat interval polytopes or into flag positroids. To all of these notions we give necessary conditions in terms of the Plcker coordinates for a valuated flag matroid to belong to such class. We conjecture that these conditions are sufficient and we look at the cases where we know this holds.

Jorge Olarte
CUNEF University, Madrid
jorge.olarte@cunef.edu

CP4

The Flag-Algebra of Rooted Binary Trees

While trees are usually considered sparse objects, they turn dense when considering only the leaves to be the ”vertices” of a tree. One can then apply the concept of inducibility of graphs, introduced in 1974 by Pippenger and Golumbic, to leaf-labeled trees. In this framework, an induced subtree is defined as the smallest tree containing a given subset of leaves, where inner vertices of degree 2 are contracted. We can then naturally extend Razborov's flag-algebras to this setting. Flag-algebras are a very powerful tool of extremal combinatorics, that have already been successfully used to tackle a large variety of problems in combinatorics and geometry. This allows the application of sums-of-squares and moment techniques to extremal questions about trees. We introduce and apply these methods to investigate problems such as the inducibility of trees, which is an important problem stemming from phylogenetics, as well as the density profiles of trees.

Diane Puges, Daniel Brosch
Alpen-Adria-Universität Klagenfurt
diane.puges@aau.at, diane.puges@aau.at

CP5

l-Intersection Pairs of Constacyclic and Conjucyclic Codes

Let C1 and C2 be two linear codes over a finite field Fq. Then (C1,C2) is an l intersection pair of codes if and only if dim(C1 nC2) = l. For l = 0 and C1 + C2 = Fnq , the definition of l intersection pair of codes stands for LCP of codes, and if C2 = C?e 1 , the definition stands for the hull of the code C1. Thus, the l intersection pair of codes generalize LCP and hull of codes. Guenda et al. introduced l-intersection pair of codes over a finite field in [1]. In that paper, they characterized l-intersection pair of codes and also demonstrated their application in constructing entanglement-assisted quantum error-correcting (EAQEC) codes. This paper focuses on the study of l-intersection pairs of constacyclic and conjucyclic codes. Specifically, we present a characterization for an l-intersection pair of constacyclic codes and obtain a condition for a linear complementary pair (LCP) of codes. We also introduce and characterize the l-intersection pair of additive conjucyclic (ACC) codes over Fq2 , where q is a prime. Similarly, we extend the definition of l- intersection pair of codes to additive codes over Fqr , where q is a prime and r is a finite positive integer. We construct some EAQEC codes.

Ramakrishna Bandi
International Institute of Information Technology Naya Raipu
ramakrishna@iiitnr.edu.in

Md Ajaharul Hossain
IIIT Naya Raipur
mdajaharul@iiitnr.edu.in

CP5

Sidon Spaces and Cyclic Subspace Codes

Sidon Spaces have been introduced by Bachoc, Serra and Zmor in 2017 as the q-analogue of Sidon sets, classical combinatorial objects introduced by Simon Szidon. A Sidon space is an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$ where the products of nonzero distinct elements are uniquely determined, up to a multiplicative factor in $\mathbb{F}_q$. The interest on Sidon spaces has increased quickly, especially after the work of Roth, Raviv and Tamo in 2018, in which they highlighted the equivalence between Sidon spaces and Cyclic subspace codes. Indeed, this class of codes, as pointed out by Koetter and Kschischang in 2008, can be used in random network coding, an encoding scheme that is capable of modelling most of nowadays applications.?Up to now, known constructions of Sidon Spaces may be classified in three families: the ones contained in the sum of two multiplicative cosets of a fixed subfield of $\mathbb{F}_{q^n}$; the ones contained in the sum of more than two multiplicative cosets of a fixed subfield of $\mathbb{F}_{q^n}$ and the ones obtained as the kernel of linearized polynomials. In this talk we will give characterization results and we will show some new examples, arising also from some well-known combinatorial objects such as scattered spaces. Moreover, we will give a quite natural definition of equivalence between Sidon spaces, which relies on the concept of equivalent cyclic subspace codes, and we will discuss about the equivalence of the known examples.

Chiara Castello
Università degli Studi della Campania ”Luigi Vanvitelli”
chiara.castello@unicampania.it

Olga Polverino
University of Campania
olga.polverino@unicampania.it

Paolo Santonastaso
University of Caserta
paolo.santonastaso@unicampania.it

Ferdinando Zullo
Università degli Studi della Campania
ferdinando.zullo@unicampania.it

CP5

Multishot Adversarial Network Decoding

Adversarial network coding studies the transmission of data over networks affected by adversarial noise. In this context, the noise is modeled by an omniscient adversary who is restricted to corrupting a subset of the network edges of a given size. A combinatorial framework for adversarial networks was introduced by Ravagnani and Kschischang and the study was recently furthered by Beemer, Kilic and Ravagnani, with particular focus on the one-shot capacity. The one-shot capacity is a measure of the maximum number of symbols that can be sent in a single use of the network without errors. In the first part of this talk we provide a general introduction to adversarial network coding and its methods. In the second part, we present the problem of studying the capacity of a network in multiple transmission rounds and some preliminaries result in this direction.

Julia Shapiro, Giuseppe Cotardo
Virginia Tech
juliams22@vt.edu, gcotardo@vt.edu

Gretchen Matthews
Virginia Tech, U.S.
gmatthews@vt.edu

Alberto Ravagnani
Eindhoven University of Technology
a.ravagnani@tue.nl

CP5

Quasi-Twisted Quantum LDPC Codes

Quasi-twisted LDPC (low-density parity-check) codes have become the leading choice among LDPC codes due to their exceptional performance. Unlike classical LDPC codes, which use sparse random matrices for code definition, QLDPC codes require a modified approach due to an orthogonality constraint. Using lifted product we construct quasi-twisted QLDPC codes: Let $\mathcal{R} \subseteq \mathbb{F}_q^{\ell \times \ell}$ be the ring of twistulant matrices, let $A \in \mathcal{R}^{m_A}$ and $B \in \mathcal{R}^{m_B}$ be block matrices defining two classical quasi-twisted codes of index m_A and m_B over $\mathcal{R}$. Then, a quantum CSS (Calderbank-Shor-Steane) code Q can be obtained with the parity-check matrices

$$H_X := [A, -B], \quad H_Z := [I_{m_A} \otimes B^\top, A^\top \otimes I_{m_B}],$$

where $A^\top = (A_1^\top, \dots, A_{m_A}^\top)$ is the intuitive transpose of a block matrix and $\otimes$ is the Kronecker product operating on two matrices of arbitrary size. Note that $H_X \cdot H_Z^\top = 0$. To control the density of the two parity-check matrices we consider the corresponding weight matrices. We then determine the dimension of such codes and give a lower bound on the distance.

Nadja Willenborg, Anna-Lena Horlemann
University of St. Gallen
nadja.willenborg@unisg.ch,
anna-lena.horlemann@unisg.ch

Martino Borello
University Paris 8
martino.borello@gmail.com

Habibul Islam
University of St. Gallen
habibul.islam@unisg.ch

CP6

High-Dimensional Causality Cone: Algebraic Foundation and Optimization

In this talk, we explore the nonconvex second-order cone (SOC) as a higher dimensional conic extension of the known causality cone in relativity and a nonconvex conic extension of the known convex SOC in mathematics and operations research. The nonconvex SOC can reformulate nonconvex quadratic programming in conic format. We define notions of its algebraic structure and show that this algebraic structure is a commutative power-associative magma whose cone of squares is the nonconvex SOC itself. We also generalize numerous algebraic properties that already exist in the convex SOC framework to the nonconvex SOC framework. Finally, we present our attempts to solve the optimization problem over the nonconvex SOC.

Baha Alzalg
Washington State University
baha2math@gmail.com

CP6

Time-Varying Semidefinite Programming: Geometry of the Trajectory of Solutions

In many applications, solutions of convex optimization problems must be updated on-line, as functions of time. We consider time-varying semidefinite programs (TV-SDP), which are linear optimization problems in the semidefinite cone whose coefficients (input data) depend on time. We are interested in the geometry of the solution (output data) trajectory, defined as the set of solutions depending on time. We propose an exhaustive description of the geometry of the solution trajectory. As our main result, we show that only 6 distinct behaviors can be observed at a neighborhood of a given point along the solution trajectory.

Antonio Bellon
CTU Prague
belloant@fel.cvut.cz

Vyacheslav Kungurtsev
Czech Technical University in Prague
Department of Computer Science
vyacheslav.kungurtsev@fel.cvut.cz

Jakub Marecek
Czech Technical University
jakub.marecek@fel.cvut.cz

Didier Henrion
LAAS-CNRS, University of Toulouse, France
and Czech Technical University in Prague, Czechia
henrion@laas.fr

CP6

Improved Nonnegativity Certification with Bernstein Polynomials

We consider the problem of certifying a polynomial on an interval is nonnegative via Bernstein polynomials. We present a simple sufficient condition that is provably less restrictive than requiring nonnegativity of all Bernstein coefficients. We generalize to matrix-valued functions of arbitrary degree.

Mitchell Harris, Pablo A. Parrilo
Massachusetts Institute of Technology
mitchh@mit.edu, parrilo@MIT.EDU

CP6

Exact Convergence Rates of Alternating Projections for the Cone of Positive Semidefinite Matri-

ces

The method of alternating projections is an algorithm for finding a point in the intersection of two sets, by iteratively projecting points to each of the two sets. The method has a variety of applications such as image recovery, phase retrieval and control theory. In addition, the method has attracted substantial research interest due to the simplicity of the algorithm. In this talk, we investigate the exact convergence rate of alternating projections for the nontransversal intersection of S_+^n and an affine space. When the affine space is a line, we show that the convergence rate is at most $O(k^{-1/2})$, independently of singularity degree of the intersection. In addition, the exact rate is linear if the matrix corresponding to the direction of the line satisfies a rank condition on its submatrix. The main tools for our analysis are the expression of the determinant of a matrix pencil by using adjugate matrices and compound matrices, and the Newton polygon associated with the characteristic polynomial. We also investigate alternating projections for S_+^3 and a three dimensional affine space in detail.

Yoshiyuki Sekiguchi
Tokyo University of Marine Science and Technology
yoshi-s@kaiyodai.ac.jp

Hiroyuki Ochiai, Hayato Waki
Kyushu University
ochiai@imi.kyushu-u.ac.jp, waki@imi.kyushu-u.ac.jp

CP7

Non-Existence of LCD MDS Group Codes Over Finite Group Algebra

The purpose of the work is to characterize support set of a generator of the LCD group code and to exhibit its importance in studying the existence and non-existence of LCD MDS group code, under specific scenarios. Linear complementary dual LCD code is a special class of code that has trivial intersection with their dual. We characterize the support of a generator of the LCD group code with a focus on the algebraic structure of the underlying group. We also explore the dimension and distance of the LCD group code under certain restrictions. The non-existence of LCD MDS group code is discussed under specific circumstances. Specifically, it is shown that there does not exist any LCD MDS group code in binary Dihedral group algebra. The utility of the results is exhibited through relevant examples.

Satya Bagchi
National Institute of Technology, Durgapur, India
satya.bagchi@maths.nitdgp.ac.in

CP7

Is χ_n a Power Function?

The map χ_n occurs in many cryptographic schemes, e.g., Keccak-f (in SHA-3 [NIST, 2015]) and ASCON [Dobraunig et al., 2021], [NIST, 2023]. The map χ_n maps bitstrings $(x_0, \ldots, x_{n-1})$ to $(y_0, \ldots, y_{n-1})$ where each $y_i = x_i + (x_{i+1} + 1)x_{i+2}$ (indices modulo n). Considering χ_n as a map of $GF(2^n)$ to itself (via $GF(2)^n \cong GF(2^n)$), this is a univariate polynomial with coefficients in $GF(2^n)$. E.g., χ_3 will be t^6 for some ordered normal basis of $GF(2^n)$. We note that χ_3 is a single monomial, thus χ_3 is a power function. In this talk, we will discuss whether χ_n is a power function for certain n. By computer experiments for χ_n ($n = 5, 7, 9, 11$), we found that none of them are a power function, regardless of the choices. We therefore investigate whether this holds for every $n > 3$. Concrete results that we have obtained: χ_n is not a power function for even n, also not for any n such that $2^n - 1$ is a prime. Furthermore, by using results about the structure of the state diagram of χ_n [Schoone and Daemen, https://ia.cr/2023/328] and power functions [Ahmad, Cycle structure of automorphisms of finite cyclic groups, 1969], we come up with several necessary conditions wherewith we can verify that χ_n is not a power function for any $3 < n < 1061$ (except $n = 441$) in a few minutes.

Jan Schoone
Radboud University Nijmegen
jan.schoone@ru.nl

CP7

Column Parity Mixers Module Theory

Circulant Column Parity Mixers (CCPMs) [Stoffelen & Daemen, 2018, p.126–159] are a class of $\mathbb{F}_q$-linear maps which are a generalization of the θ mixing layers in well-known cryptographic primitives like SHA-3 [Bertoni et al., 2015, p.389]. They provide a good trade-off between implementation cost and mixing power, making them well suited for lightweight cryptography. Surprisingly, not much is known regarding their algebraic properties, which might be due to the complexity of defining CCPMs in terms of linear algebra. A new approach is introduced, where we reintroduce CCPMs as endomorphisms of free R-modules, where $R = \mathbb{F}_q[G]$ for some finite Abelian group G. This implies that CCPMs can be considered as a class of square matrices with entries in R. Many non-trivial previous observations now reoccur as trivial consequences of module-theoretic concepts. Take for example the invertibility criterion of CCPMs. A new result using this approach is a criterion whether a CCPM admits an eigenbasis, which depends on the structure of R. Interestingly, the proof of the criterion requires localization of R together with Nakayama's Lemma, which is a nice example of applying non-trivial concepts from commutative algebra to study CCPMs. Moreover, this module-theoretic approach is very suitable for designing CCPMs with a high order, which is relevant against invariant subspace attacks [Beierle et al., 2017, p.647–678].

Robert Christian Subroto
Radboud University
bobby.subroto@ru.nl

CP7

A New Exact Algebraic Method for Multi-Objective Linear Integer Programming

We introduce a new exact algorithm for obtaining a minimal set of efficient solutions of a multi-objective linear integer problem $\min c_1(\mathbf{x}), \ldots, c_p(\mathbf{x})$ s.t. $A\mathbf{x} = \mathbf{b}$, $\mathbf{x} \in \mathbb{Z}^n_{\geq 0}$. For this purpose we use the classical ϵ-constraint method that manage some auxiliary problems P_i with only one objective function c_i and additional constraints $c_j(\mathbf{x}) \leq \epsilon_j$ for $i \neq j$ for some suitable $\epsilon_j \in \mathbb{R}$. Our approach exploid the properties of test sets associated to a linear integer problem (computed with Gröbner bases). Test sets identify a considerable number of useless P_i, avoiding unnecessary computations. This work is a generalization of the biobjective case presented in European J. Oper. Res., 282(2):453463, 2020.

Jose M. Ucha

Departamento de Matematica Aplicada I
Universidad de Sevilla (Spain)
ucha@us.es

María Isabel Hartillo
Universidad de Sevilla
hartillo@us.es

jiménez-Tafur Haydee
Universidad Pedagógica Nacional
hjimenezt@pedagogica.edu.co

CP8

Maximal Persistence in Random Clique Complexes

In this talk, we explore the persistent homology of an Erdos-Renyi random clique complex filtration on n vertices. Here, each edge e appears independently at a uniform random time $p_e \in [0,1]$, and the persistence of a cycle σ is defined as $p_2(\sigma)/p_1(\sigma)$, where $p_1(\sigma)$ and $p_2(\sigma)$ are the birth and death times of σ. We show that if $k \geq 1$ is fixed, then with high probability the maximal persistence of a k-cycle is of order $n^{1/k(k+1)}$.

Ayat A. Ababneh
The university of Jordan
a.ababneh@ju.edu.jo

CP8

Gluing Elliptic Curves Along the 3-Torsion

I present a method for constructing hyperelliptic curves C of genus two that are triple covers of two given elliptic curves E and E' from the Hesse pencil, as well as constructing an explicit $(3,3)$-isogeny $E \times E' \to \mathrm{Jac}(C)$. The method generalizes to degree-n covers of elliptic curves with n-level structure for odd n, but it is computationally expensive. The case $n = 3$ may be of interest as the first step in attacking SIDH via $(3,3)$-descent, in a manner analogous to the recent work of Castryck and Decru.

Martin Djukanovic
Groningen
martin.djukanovic@pm.me

CP8

Orthogonal and Linear Regression, Moments of Inertia, Confocal Quadrics, and Billiards

We emphasize the importance of bridges between statistics, mechanics, and geometry. We develop and employ links between pencils of quadrics, moments of inertia, and linear and orthogonal regressions. For a given system of points in R^k representing a sample of a full rank, we construct a pencil of confocal quadrics which appears to be a useful geometric tool to study the data. Some of the obtained results can be seen as generalizations of classical results of Pearson on orthogonal regression. Applications include statistics of errors-in-variables models (EIV) and restricted regressions, both ordinary and orthogonal ones. For the latter, a new formula for test statistic is derived. The developed methods and results are illustrated in natural statistics examples. We discuss applications in mechanics, including integrable billiard dynamics.

Vladimir Dragovic
The University of Texas at Dallas
vlad.dragovic@gmail.com

Borislav Gajic
Mathematical Institute SANU, Belgrade
gajab@mi.sanu.ac.rs

CP8

Topology of Configuration Spaces of Mechanical Linkages

We present an approach to the study of configuration spaces of mechanical linkages and its several applications to spider linkages. Our approach is based on the investigation of the fibers of real quadratic mappings of the distance-squared type naturally associated with linkages considered. To this end we develop an algorithm for computing the bifurcation diagram and Euler characteristics of the fibers of a distance-squared mapping based on the signature formula for the Euler characteristic given in our earlier papers. This enables us to compute the Euler characteristic of configuration space of spider linkage with the branches consisting of two links and develop an algorithm of robust Coulomb control in the spirit of [G. Khimshiashvili, D. Siersma, Hooke and Coulomb energy of a tripod spider. Proc. I. Vekua Inst. Appl. Math. 72(2022), 20-33], [G. Khimshiashvili, D. Siersma, Hooke and Coulomb Energy of Tripod Spiders. ArXiv:2301.09314.]. In conclusion we will mention several open problems and further feasible applications suggested by our approach.

Giorgi Khimshiashvili
Ilia State University, Tbilisi, Georgia
Ilia State University, Tbilisi, Georgia
giorgi.khimshiashvili@iliauni.edu.ge

MS1

A New Algebraic Approach to the Regular Syndrome Decoding Problem and Implications for PCG Constructions

The Regular Syndrome Decoding (RSD) problem, a variant of the Syndrome Decoding problem with a particular error distribution, was introduced almost 20 years ago by Augot et al.. In this problem, the error vector is divided into equally sized blocks, each containing a single noisy coordinate. More recently, the last five years have seen increased interest in this assumption due to its use in MPC and ZK applications. Generally referred to as ”LPN with regular noise” in this context, the assumption allows to achieve better efficiency when compared to plain LPN. In all previous works of cryptanalysis, it has not been shown how to exploit the special feature of this problem in an attack. We present the first algebraic attack on RSD. Based on a careful theoretical analysis of the underlying polynomial system, we propose concrete attacks that are able to take advantage of the regular noise distribution. In particular, we can identify several examples of concrete parameters where our techniques outperform other algorithms. (joint work with Morten ygarden)

Pierre Briaud
INRIA
pierre.briaud@inria.fr

MS1

Cryptanalysis of HFEv-

HFEv- schemes is a multivariate scheme. It was submitted to the NIST post-quantum cryptography competition in the name of GeMMS. It was considered a very secure though not very efficient scheme with nearly 20 years of history and it was a NIST third round PQC candidate. In this talk,we will present the MinRank attack that breaks completely the HFEv- schemes. This work won honorable mention for the best paper award in crypto 2021.

Jintai Ding
University of Cincinnati
jintai.ding@gmail.com

MS1

Refined F5 Algorithms for Ideals of Minors of Square Matrices

Let k a field, M an nXn matrix of linear forms over k and an integer r smaller than n. The MinRank problem asks to compute the set of points p in an algebraic closure of k such that the evaluation of M at p has rank at most r. This set is equivalent to vanishing set of the ideal I(M,r) generated by the (r+1)-minors of M. The MinRank problem arises in effective real algebraic geometry and more recently in cryptography in pursuit of quantum safe cryptography schemes. Several post-quantum cryptosystems (e.g. HFE) rely on the difficulty of the MinRank problem. The ideal I(M,r) cannot be generated by a regular sequence. Thus, reductions to zero appear when running the F5 algorithm to compute a grevlex Groebner basis of I(M,r), regardless of the generators chosen for I(M,r). Using results on the first syzygy module of I(M,r), we introduce a new criterion which predicts reductions to zero when computing a Groebner basis for I(M,r). We remove these reductions to zero, thereby speeding up the Groebner basis computation. Experimental data indicates an improvement on the best-known complexity bound for Groebner basis solutions to the MinRank problem. In the case r=n-2, we exploit a known free resolution of I(M,r) given by Gulliksen and Negard to refine our criterion and avoid all reductions to zero. We show that the complexity of our new algorithm improves on best-known bounds for Groebner basis solutions to the MinRank problem. Joint work with Vincent Neiger and Mohab Safey El Din.

Sriram Gopalakrishnan
LIP6
sriram.gopalakrishnan@lip6.fr

MS2

On Permutation Groups of Some Evaluation Codes

The permutation group of a code is the set of permutations of entries that keep the code invariant. For evaluation codes, an interesting subfamily of the permutation group is the affine permutation group, that are the permutations that can be seen as affine transformations of the set of evaluation points. We study some properties of the affine permutation group in the case of decreasing codes. These include the well-known case of Reed-Muller case and the recently described polar codes over binary symmetric channels.

Eduardo Camps Moreno, Hiram H. Lopez
Cleveland State University
e.camps@csuohio.edu, h.lopezvaldez@csuohio.edu

Eliseo Sarmiento
Instituto Politécnico Nacional
esarmiento@ipn.mx

Ivan Soprunov
Cleveland State University
Department of Mathematics
i.soprunov@csuohio.edu

MS2

Locally Recovered Codes with Availability and Hierarchy from Fiber Products

Curves (or higher dimensional varieties) over finite fields have rich geometric structure that can lead to natural constructions of codes with locality, availability, and hierarchy. This talk will discuss how locally recoverable codes with availability from fiber products of curves are also endowed with a hierarchical recovery structure, and connect these codes with more general geometric constructions.

Beth Malmskog
Colorado College
beth.malmskog@gmail.com

MS2

Locally Recoverable Codes from Towers of Function Fields

In this work, we construct sequences of locally recoverable AG codes arising from a tower of function fields and giving bounds for the parameters of the obtained codes. In a particular case of a tower over $\mathbb{F}_{q^2}$ for any odd q power of a prime, defined by Garcia and Stichtenoth, we show that the bound is sharp for the first code in the sequence, and we include a detailed analysis for the following codes in the sequence based on the distribution of rational places that split completely in the considered function field extension.

Maria Chara, Francisco Galluccio
Universidad Nacional del Litoral
mchara@santafe-conicet.gov.ar, frangallu996@gmail.com

Edgar Martinez-Moro
Institute of Mathematics
University of Valladolid
edgar.martinez@uva.es

MS2

Gaps and Pure Gaps Sets in Weierstrass Semigroups

In this talk we will consider the problem of determining Weierstrass gaps and pure Weierstrass gaps at several points. Using the notion of relative maximality in generalized Weierstrass semigroups due to Delgado, we present a description of these elements which generalizes the approach of Homma and Kim given for pairs. Through this description, we present a study of the gaps and pure gaps at several points on a certain family of curves with separated variables.

Guilherme Tizziotti
Universidade Federal de Uberlândia
guilhermect@ufu.br

MS3

Rank-Metric Codes and q-Matroids: A Decomposition of q-Matroids Into Irreducible Components

q-Matroids, the q-analogue of matroids, have been intensively studied due to their connection with rank metric codes. For both matroids and q-matroids, it is possible to construct new (q-)matroids via the direct sum operation. For the classical matroid case, much of the structure of the direct sum (such as its flats, independent sets, basis) can be nicely characterized in terms of the structure of the summands. However, in general, the same does not hold true for q-matroids. Luckily, it is still possible to fully characterize the cyclic flats of the direct sum of q-matroids from the cyclic flats of each of the summands. Furthermore, I will show in my talk that one can use the cyclic flats of a q-matroid to determine if the q-matroid is irreducible, meaning it is not the direct sum of two ”smaller” q-matroids. This will then allow me to show that q-matroids can be uniquely decomposed (up to equivalence) into the direct sum of irreducible q-matroids.

Benjamin Jany, Heide Gluesing-Luerssen
University of Kentucky
bja246@uky.edu, heide.gl@uky.edu

MS3

High Degree Symmetric Rank-Metric Codes

Over fields of characteristic different from 2, symmetric matrices can be identified with degree 2 homogeneous polynomials. This allows us to view symmetric rank-metric codes as living inside the space of such polynomials. In this talk, we extend the study of symmetric rank-metric codes to higher degree of symmetry. We equip the space of homogeneous polynomials of degree d with the metric induced by the essential rank, which is the minimal number of linear forms needed to express a polynomial. In this context, we generalize the construction of symmetric Gabidulin codes to polynomials of degree d over field of characteristic 0 or larger than d.

Arthur Bik
Institute for Advanced Studies
mabik@ias.edu

Alessandro Neri
Ghent University
alessandro.neri@ugent.be

MS3

Asymptotics of the Etzion-Silberstein Conjecture

This talk focuses on rank-metric codes supported on a Ferrers diagram, i.e., linear spaces of matrices over a finite field in which the non-zero entries of each matrix lie on a Ferres diagram. I will describe the role played by these codes in network coding and discuss a wide open problem in the field, namely the Etzion-Silberatein conjecture, as well as its asymptotic version as the field size approaches infinity. I will then present new results connecting said conjecture with the theory of q-rook polynomials of Ferrers diagrams.

Anina Gruica, Alberto Ravagnani
Eindhoven University of Technology
a.gruica@tue.nl, alberto.rvgn@gmail.com

MS3

Positivity Properties of Q-Hit Numbers of the Finite General Linear Group

We consider the problem of counting matrices over a finite field with fixed rank and support contained in a fixed set. The count of such matrices gives a q-analogue of the classical rook number, although it is not-polynomial in general. Lewis and Morales defined a corresponding q-analogue of hit numbers, and conjectured several positivity properties for them. We find explicit formulas for the residues of q-hit numbers in low degrees, and prove these residues are non-negative, partially answering one of their conjectures.

Jeffrey Chen
University of Chicago Laboratory Schools
jeffreychen51@gmail.com

Jesse Selover
University of Massachusetts Amherst
jselover@umass.edu

MS4

Mbius Transform Based Bounds for Constant Weight Codes

A popular method for obtaining upper bounds on the size of error-correcting codes is to first reformulate the problem as an (integer) optimization problem, and then relax it to a semidefinite programming problem. Any feasible solution of the dual of such a relaxation gives an upper bound on the size of the corresponding class of codes. The main problem of this approach is the size of the relaxation, usually requiring technical representation theoretic arguments (specific to the case) to exploit the symmetries of the relaxations to make them computationally feasible. We propose a new hierarchy of semidefinite relaxations for constant weight codes, which, in contrast to more usual Lasserre-style relaxations, allow for near-trivial symmetry reductions. To do this we generalize ideas coming from Razborov's flag algebras, and focus on Mbius transforms to reduce the size of the optimization problem.

Daniel Brosch
Alpen-Adria-Universität Klagenfurt
daniel.brosch@aau.at

Sven C. Polak
CWI
s.c.polak@tilburguniversity.edu

MS4

Hyperbolic Polynomials and Starved Polytopes

Inspired by a proof of Timofte's degree and half degree principle for symmetric polynomials, we study sets of univariate hyperbolic polynomials that share the same first few coefficients. We show that the various root arrangements of hyperbolic polynomials, together with a natural partial order, can be used to describe the geometry of these sets in much the same way as one can describe a polytope in terms of its face lattice. In particular, when we stratify our sets of hyperbolic polynomials in terms of the possible root arrangements, we will see that the poset of strata makes a graded, atomic and coatomic lattice. This observation results in an algorithm to compute which root arrangements are realized based solely on the (finite) collection of zero dimensional strata. Together with some nice geometrical properties of the strata, this combinatorial description justifies describing these sets as ”starved polytopes”.

Arne Lien
University of Konstanz

arne.lien@uni-konstanz.de

MS4
When is an Odd Power of a psd Form sos?

In 1979, Stengle constructed a psd ternary sextic form T with the property that for each positive integer $2k+1$, T^{2k+1} is not sos; that is, T^{2k+1} cannot be written as a sum of squares of forms. It turns out this is also true for the Motzkin form M and some other extremal psd forms. On the other hand, in 2012, Scheiderer proved that if p is positive definite, then for sufficiently large k, p^{2k+1} is sos. We will discuss the current understanding of these phenomena, and give examples of forms p where p is not sos, but p^3 is sos.

Bruce Reznick
University of Illinois at Urbana-Champaign
reznick@math.uiuc.edu

MS5
Positivity Problems in Reaction Network Theory

Systems of polynomial equations and inequalities arise naturally when studying properties of the steady states biochemical reaction networks. In this setting, the relevant steady states are the positive solutions of a system of polynomial equations with parametric coefficients. In one specific scenario, the study of the signs a (typically large) polynomial attains over the positive orthant, is enough to determine whether the system of steady states admits more than one positive solution for some choice of parameter values. Furthermore, parameter regions where this occurs can be determined by employing ideas from the theory of sums of nonnegative circuits. Although the framework arises from the study of reaction networks, the mathematical theory is independent of this. In this talk, I will explain how the relevant polynomial is constructed, discuss its properties and how to analyse it, and throughout present examples from the context of reaction networks. This talk will combine results from several join works with: Conradi, Curiel, Henriksson, Kaihnsa, Mincheva, Telek, Yrck, Wiuf, de Wolff.

Elisenda Feliu
University of Copenhagen
efeliu@math.ku.dk

MS5
Optimal Experimentation for Learning Personalized Policies Across Locations

Firms wish to learn personalized policies for customers in heterogeneous yet related locations to maximize their monetary gains. To do this, they conduct experiments at each location to estimate the parameters of a customer response function. A key decision is which action to assign to each participant in the experiment, especially when a participant can only be assigned one action, or there are budget constraints. The existing experimentation methodology considers locations and experiments individually. In this work, we leverage the relationship between locations in the experimentation problem to learn more profitable policies by proposing novel estimators and a semidefinite programming approach. Joint work with Stefanos Poulidis and Spyros Zoumpoulis

Georgina Hall
INSEAD
georgina.hall@insead.edu

MS5
Polynomial Argmin for Recovery and Approximation of Multivariate Discontinuous Functions

We propose to approximate a (possibly discontinuous) multivariate function $f(x)$ on a compact set by the partial minimizer argmin_y $p(x,y)$ of an appropriate polynomial p whose construction can be cast in a univariate sum of squares (SOS) framework, resulting in a highly structured convex semidefinite program. In a number of non-trivial cases (e.g. when f is a piecewise polynomial) we prove that the approximation is exact with a low-degree polynomial p. Our approach has three distinguishing features: (i) It is mesh-free and does not require the knowledge of the discontinuity locations. (ii) It is model-free in the sense that we only assume that the function to be approximated is available through samples (point evaluations). (iii) The size of the semidefinite program is independent of the ambient dimension and depends linearly on the number of samples. We also analyze the sample complexity of the approach, proving a generalization error bound in a probabilistic setting. This allows for a comparison with machine learning approaches.

Didier Henrion
LAAS-CNRS, University of Toulouse, France
and Czech Technical University in Prague, Czechia
henrion@laas.fr

Milan Korda
LAAS-CNRS in Toulouse,
Czech Technical University in Prague
mkorda@laas.fr

Jean B. Lasserre
LAAS CNRS and Institute of Mathematics
lasserre@laas.fr

MS5
Lower Bounds on Neural Network Depth via Lattice Polytopes

We study the set of functions representable by ReLU neural networks, a standard model in the machine learning community. It is an open question whether this set strictly increases with the number of layers used. We prove that this is indeed the case if one considers neural networks with only integer weights. We show that at least log(n) many layers are required to compute the maximum of n numbers, matching known upper bounds. To obtain our result, we first use previously discovered connections between neural networks and tropical geometry to translate the problem into the language of Newton polytopes. These Newton polytopes are lattice polytopes arising from alternatingly taking convex hulls and Minkowski sums. Our depth lower bounds then follow from a parity argument for the volume of faces of such polytopes, which might be of independent interest. This is joint work with Christian Haase and Christoph Hertrich.

Georg Loho
University of Twente
g.loho@utwente.nl

Christian Haase
FU Berlin
haase@math.fu-berlin.de

Christoph Hertrich
LSE
c.hertrich@lse.ac.uk

MS6

Density Estimation Using Hit and Run Sampling from the Space of Phylogenetic Trees

In this presentation we introduce a Markov Chain Monte Carlo (MCMC) Hit and Run (HAR) uniform sampler over a tropically convex space of ultrametrics. This is particularly important because by sampling from the space of ultrametrics, we are sampling from the space of phylogenetic trees, or tree space. This has wide ranging implications to statistical inference relating to this tree space. Specifically, we show how this HAR sampler can be employed to sample over the space of ultrametrics in order to non-parametrically estimate the phylogenetic tree distribution using what we call tropical density estimator (TDE) with the tropical metric. We compare the results of the TDE using the tropical metric against often used density estimation methods using the Billera-Holmes-Vogtman metric to show that TDE is more accurate and computationally less expensive.

David Barnhill, Ruriko Yoshida
Naval Postgraduate School
david.barnhill@nps.edu, ryoshida@nps.edu

Keiji Miura
Kwansei Gakuin University
miura@kwansei.ac.jp

MS6

Algebraic Invariants in Linear (Convolutional) Neural Networks

A common optimization strategy within machine learning with neural networks is variations of gradient descent. Typically, the gradient flow curves are not algebraic. However, they do satisfy non-trivial algebraic invariants, meaning that each gradient flow curve is contained in a proper irreducible Zariski closed set (whose dimension is typically larger one). Those invariants have become important in practice to initialize neural networks in a balanced way such that gradient descent neither converges to zero nor infinity. In this talk, we describe the algebraic invariants of gradient flow for linear fully-connected networks and linear convolutional networks. This talk is based on joint works with Joan Bruna, Thomas Merkh, Guido Montfar, Vahid Shahverdi, and Matthew Trager.

Kathlen Kohn
KTH
kathlen@kth.se

MS6

Introduction to the Minimsymposium

Algebraic invariants provide useful insights into data and have been used in machine learning, statistical estimation, phylogenetics, reaction networks, and optimization among other fields. In this talk we will summarise the recent developments in the field that will be discussed in detail during the minisymposium.

Olga Kuznetsova
Aalto University
olga.kuznetsova@aalto.fi

MS7

Apolarity and the Geometry of the Decompositions of Tensors

I will discuss the interplay between the apolar ideal of a symmetric tensor (form) and the geometry of its decompositions, considered as finite sets in a projective space, in order to determine properties of the form itself, and also properties of a natural stratification of the corresponding secant varieties.

Luca Chiantini
Universita di Siena
luca.chiantini@unisi.it

MS7

Identifiability and Singular Locus of Secant Varieties to Grassmannians

In this work we determine the singular locus of the secant variety of lines to the Grassmannian $Gr(k, V)$ of k-planes in a complex vector space V, using its structure as $SL(V)$-variety: we exhibit the orbits and we study their dimensions and the inclusions among their closures. We solve the problems of identifiability and tangential-identifiability of points in the secant variety: as a consequence, we also determine the second Terracini locus to a Grassmannian.

Vincenzo Galgano
Universita di Trento, Italy
vincenzo.galgano@unitn.it

Reynaldo Staffolani
currently unaffiliated
reynaldo.staffolani@gmail.com

MS7

(Partially) Symmetric Rank of Reducible Cubics and Quartics

A famous example by Shitov shows that the rank and symmetric rank of a cubic may differ. However, we do not know what happens in between the two. Is the symmetric rank always equal to the partially symmetric rank? We prove that this is true for reducible cubics in any number of variables, and we extend this result to a family of reducible quartics.

Francesco Galuppi
Polish Academy of Sciences
fgaluppi@impan.pl

MS7

The Symmetric Geometric Rank of Symmetric Tensors

Inspired by recent work of Kopparty-Moshkovitz-Zuiddam and motivated by problems in combinatorics and hypergraphs, we introduce the notion of symmetric geometric rank for a symmetric tensor. We first derive fundamental properties of the symmetric geometric rank. Then, we study spaces of symmetric tensors with prescribed symmetric geometric rank. These turn out to be spaces of homogeneous polynomials whose corresponding hypersurfaces have a singular locus of bounded codimension.

Julia Lindberg
University of Texas-Austin
julia.lindberg@math.utexas.edu

Pierpaola Santarsiero
University of Trento
pierpaola.santarsiero@mis.mpg.de

MS8
On Some Orthogonalization Schemes in Tensor Train Format

In the framework of tensor spaces, we consider orthogonalization kernels to generate an orthogonal basis of a tensor subspace from a set of linearly independent tensors. In particular, we investigate numerically the loss of orthogonality of six orthogonalization methods, namely Classical and Modified Gram-Schmidt with (CGS2, MGS2) and without (CGS, MGS) re-orthogonalization, the Gram approach, and the Householder transformation. To tackle the curse of dimensionality, we represent tensor with low rank approximation using the Tensor Train (TT) formalism, and we introduce recompression steps in the standard algorithm outline through the TT-rounding method at a prescribed accuracy. After describing the algorithm structure and properties, we illustrate numerically that the theoretical bounds for the loss of orthogonality in the classical matrix computation round-off analysis results are maintained, with the unit round-off replaced by the TT-rounding accuracy. The computational analysis for each orthogonalization kernel in terms of the memory requirement and the computational complexity measured as a function of the number of TT-rounding, which happens to be the computational most expensive operation, completes the study.

Olivier Coulaud
INRIA
olivier.coulaud@inria.fr

Luc Giraud
Inria
luc.giraud@inria.fr

Martina Iannacito
KU Leuven
martina.iannacito@kuleuven.be

MS8
Any-Dimensional Convex Sets

Classical algorithms are defined on inputs of different sizes. In contrast, algorithms learned from data may only be defined on inputs of the same size as the data. What does it mean for an algorithm to be defined on infinitely-many input sizes? How do we describe such algorithms, and how do we parametrize and search over them? In this talk, we tackle these questions for convex optimization-based algorithms. Describing such algorithms reduces to describing convex sets. These, in turn, are often ”freely” described, meaning that their description makes instantiation in every dimension obvious. Examples include unit balls of standard norms defined on vectors of any size, graph parameters defined for graphs of any size, and (quantum) information theoretic quantities defined for distributions on any number of (qu)bits. We show that such free descriptions of convex sets arise from two ingredients. First, group invariance and the recently-identified phenomenon of representation stability. Second, embeddings and projections relating different-sized problem instances. We combine these ingredients to obtain parametrized families of infinitely instantiable convex sets. To extend a set learned from data in a fixed dimension to higher ones, we identify consistency conditions relating sets in different dimensions that are satisfied in a variety of applications, and obtain parametrizations respecting these conditions.

Eitan Levin
Caltech
eitanl@caltech.edu

Venkat Chandrasekaran
California Institute of Technology
venkatc@caltech.edu

MS8
First-Order Optimization on Stratified Sets

We consider the problem of minimizing a differentiable function with locally Lipschitz continuous gradient on a stratified set, and present a first-order algorithm designed to find a stationary point of that problem. Our assumptions on the stratified set are satisfied notably by the set of nonnegative sparse vectors, the determinantal variety (i.e., matrices of bounded rank), and its intersection with the cone of positive-semidefinite matrices. The iteration map of the proposed algorithm applies a step of projected projected gradient descent with backtracking line search, as proposed by Schneider and Uschmajew (2015), to its input but also to a projection of the input onto each of the lower strata from which it is considered close, and outputs a point among those thereby produced that reduces the cost function the most. Under our assumptions on the stratified set, we prove that this algorithm produces a sequence of iterates whose accumulation points are stationary, and therefore does not follow the so-called apocalypses described by Levin, Kileel, and Boumal (2022). We illustrate the apocalypse-free property of our method through a numerical experiment on the determinantal variety.

Guillaume Olikier
Université catholique de Louvain
guillaume.olikier@uclouvain.be

Pierre-Antoine Absil
Université Catholique de Louvain
ICTEAM Institute
pa.absil@uclouvain.be

Kyle Gallivan
Florida State University
gallivan@math.fsu.edu

MS8
Protes: Probabilistic Optimization with Tensor Sampling

We develop new method PROTES for optimization of the multidimensional arrays and discretized multivariable functions, which is based on a probabilistic sampling from a probability density function given in the low-parametric tensor train format. We tested it on complex multidimensional arrays taken, among other, from real-world applications, including unconstrained binary optimization and optimal control problems, for which the possible number of elements is up to 2^{100} elements. In numerical experiments, both on analytic model functions and on complex problems, our algorithm outperform existing popular discrete optimization methods (Particle Swarm Optimization, Covariance Matrix Adaptation, Differential Evolution and others). Moreover, we take the same set of hyperparameters of our algorithm for all numerical applications.

Ivan Oseledets
Skolkovo Institute of Science and Technology
ivan.oseledets@gmail.com

MS9

On the Typical and Atypical Solutions to the Kuramoto Equations

The Kuramoto model is a dynamical system that models the interaction of coupled oscillators. There has been much work to effectively bound the number of equilibria to the Kuramoto model for a given network. By formulating the Kuramoto equations as a system of algebraic equations, we first relate the complex root count of the Kuramoto equations to the combinatorics of the underlying network by showing that the complex root count is generically equal to the normalized volume of the corresponding adjacency polytope of the network. We then give explicit algebraic conditions under which this bound is strict and show that there are conditions where the Kuramoto equations have infinitely many equilibria.

Julia Lindberg
University of Texas-Austin
julia.lindberg@math.utexas.edu

MS9

Structured Root Finding via Eigenvalues: Beyond Toric Varieties

Many computer algebra methods for solving polynomial equations take into account the sparsity of the equations in the monomial basis. Toric varieties arise naturally in this context, as seen in the theory of sparse resultants. In this talk, I will go beyond toric varieties and explain eigenvalue methods which exploit Khovanskii bases. In examples, I will show how to solve equations on Grassmannians and del Pezzo surfaces.

Simon Telen
MPI Leipzig
simon.telen@mis.mpg.de

Barbara Betti, Marta Panizzut
MPI MiS Leipzig
barbara.betti@mis.mpg.de, marta.panizzut@mis.mpg.de

MS9

Introduction

This talk will introduce the minisymposium.

Elias Tsigaridas
Inria Paris
elias.tsigaridas@inria.fr

MS9

About the Fundamental Subspaces of the Macaulay Matrix

The Macaulay matrix is one of the most important matrices in algebraic geometry, where it plays a key role in elimination theory (i.e., when eliminating variables via resultants) and in polynomial system solving (e.g., when setting-up multiplication matrices). In this presentation, we will take a closer look at the (rectangular) Macaulay matrix and its fundamental subspaces. We will approach this topic from a linear algebra point of view, keeping an eye on numerical algorithms. A central role will be given to the fundamental theorem of linear algebra, connecting these vector spaces. The Macaulay matrix has four fundamental subspaces, each with an interesting interpretation in terms of the algebraic properties of the associated system of multivariate polynomials: its right null space and column space yield the common roots of that system, the row space contains the consequences of the related homogeneous ideal, and the left null space corresponds to the syzygies generated by the associated system. This presentation will demonstrate how to leverage the fundamental subspaces of the Macaulay matrix via existing (numerical) linear algebra tools to address some basic problems from algebraic geometry. The discussion will also touch upon the system-theoretic interpretation of the null space of the Macaulay matrix as the column space of the observability matrix of a descriptor system, enabling the link between polynomial root-finding and multidimensional realization theory.

Christof Vermeersch
KU Leuven
christof.vermeersch@esat.kuleuven.be

MS10

Prospects for Applications of Magnitude Homology to Cybersecurity, Network Science, and Machine Learning

Magnitude homology is a natural tool to characterize directed graphs that have compositionally coherent data attached to arcs. Such structures are commonplace–or perhaps more interestingly, may have enriched variants that can be synthesized–in applications to cybersecurity, network science, and machine learning. We briefly introduce the mechanics of magnitude homology before showing some examples and discussing prospects for near-term applications.

Steve Huntsman
Category Capital
sch213@nyu.edu

MS10

Magnitude Cohomology of Graphs

While magnitude homology has received a great deal of recent attention, magnitude *co*homology has yet to catch up. The theory of magnitude cohomology is due to Richard Hepworth (*Mathematische Zeitschrift* 301 (2022), 3617–3640). It is defined in the wide generality of enriched categories and specializes to metric spaces and, therefore, graphs. Like many cohomology theories, it has more structure than its homological counterpart. In particular, there is a cup-like product, which, however, may not be commutative if the enriching category is not cartesian. Hepworth proves the very striking result that a metric space is completely determined up to isometry by its magnitude cohomology (seen as a graded ring), provided that the space is sufficiently discrete: there is a lower bound on the set of nonzero distances. Since graphs are discrete in this sense, magnitude cohomology defines an embedding of the class of graphs into the class of graded rings. I will give an overview of the world of magnitude cohomology, concentrating on the case of graphs.

Tom Leinster
University of Edinburgh, UK
tom.leinster@ed.ac.uk

MS10
Eulerian Magnitude Homology

Hepworth, Willerton, Leinster and Shulman introduced magnitude homology groups for enriched categories, and in particular for graphs. Although the construction of the boundary map suggests magnitude homology groups are strongly influenced by graph substructures it is not straightforward to detect such subgraphs. In this talk, we introduce *eulerian* magnitude homology and show how it enables a more accurate analysis of graph substructures. We then apply these results to Erdos-Renyi random graphs and random geometric graphs, and obtain an asymptotic estimate for the Betti numbers of the eulerian magnitude homology groups on the diagonal.

Giuliamaria Menara
Università degli Studi di Trieste
giuliamaria.menara@phd.units.it

MS10
Magnitude and Magnitude Homology of Graph Gluings

Theorems which describe the behaviour of graph (or network) invariants under gluing operations have both theoretical valuefor instance, in guiding us towards axiomatic characterizationsand practical value, allowing for efficiencies to be made in computations. This talk will discuss several recent results of this type. We will see, by homological means, that the magnitude of an undirected graph is preserved under a certain ‘twisting operation, and we will discuss two new Mayer–Vietoris-type theorems describing how the magnitude homology of a directed graph may be determined by those of its subgraphs. This is partly based on work-in-progress in collaboration with Richard Hepworth; we will also draw on recent work by Yasuhiko Asao which links magnitude homology in a fundamental way to the path homology of directed graphs.

Emily Roff
University of Edinburgh, UK
emily.roff@ed.ac.uk

MS11
Algebraic Geometry at Sea

Smooth algebraic curves give rise to solutions to the KP equation, which models waves in shallow water, via Riemanns theta function. Singular curves produce solutions as well, but the theta function in this case becomes degenerate. I will present some theoretical and computational results on this topic, based on both smooth and singular curves.

Daniele Agostini
Eberhard Karls Universität Tübingen
daniele.agostini@uni-tuebingen.edu

MS11
Rational Solutions of the KP Hierarchy from Singular Algebraic Curves

This talk will report on joint work with Daniele Agostini and Trk zlum elik. We study the ”algebraic theta functions” obtained from certain singular curves in the case when the generalized Jacobian is $\mathbb{C}^g$ and the implicit equation of the theta divisor is a polynomial equation. We give a characterization of the singular curves whose theta functions have this form and show how the degree of the polynomial defining the theta divisor is determined by the combinatorial information derived from the singularities. Our main interest in this situation is that these polynomials are closely related to a class of tau functions for the Kadomtsev-Petviashvili (KP) hierarchy, generalizing the KP non-linear wave equation in two space variables. As in the KdV case, the KP equation has interesting soliton solutions, as well as other solutions generated from theta functions from smooth algebraic curves. This work provides an extensive collection of rational function solutions of the KP equation derived from singular algebraic curves as well. The tools we use rely on Mikio Sato’s algebraic approach to solutions of the KP hierarchy and makes interesting connections with combinatorial topics such as partitions and Schur polynomials.

John B. Little
College of the Holy Cross
jlittle@holycross.edu

Daniele Agostini
Eberhard Karls Universität Tübingen
daniele.agostini@uni-tuebingen.edu

Türkü zlüm elik
Simon Fraser University
turkuozlum@gmail.com

MS11
KP Solutions from Nodal Curves and the Schottky Problem

The study of solutions to the Kadomtsev-Petviashvili (KP) equation yields interesting connections between integrable systems and algebraic curves. In this talk, I will discuss solutions to the KP equation whose underlying algebraic curves undergo tropical degenerations. In these cases, Riemanns theta function becomes a finite exponential sum supported on a Delaunay polytope. I will introduce the Hirota variety which parametrizes KP solutions arising from such a sum. I will then discuss a special case: the Hirota variety associated to a rational nodal curve. Of particular interest is an irreducible subvariety that is the image of a parameterization map. Proving that this is a component of the Hirota variety entails solving a weak Schottky problem for rational nodal curves. This talk is based on joint works with Daniele Agostini, Claudia Fevola, and Bernd Sturmfels.

Yelena Mandelshtam
UC Berkeley
yelenam@berkeley.edu

Daniele Agostini
Eberhard Karls Universität Tübingen
daniele.agostini@uni-tuebingen.edu

Claudia Fevola
Max Planck Institute for Mathematics in the Sciences
claudia.fevola@mis.mpg.de

Bernd Sturmfels
MPI Leipzig and UC Berkeley
bernd@mis.mpg.de

MS11

Numerical Reconstruction of Curves From Their Jacobians

We approach the Torelli problem of reconstructing a curve from its Jacobian from a computational point of view. Following Dubrovin, we design machinery to solve this problem effectively, which builds on methods in numerical algebraic geometry. We verify these methods via numerical experiments with curves up to genus 7.

Türkü zlüm elik
Simon Fraser University
turkuozlum@gmail.com

Daniele Agostini
Eberhard Karls Universität Tübingen
daniele.agostini@uni-tuebingen.edu

Demir Eken
Bilkent University
demir.eken@ug.bilkent.edu.tr

MS12

Degenerations of the Grassmannian via Matroidal Subdivisions of the Hypersimplex

We study initial degenerations of the (3,8)-Grassmannian. Degenerations of this kind come from a term order induced by a weight vector in the tropical Grassmannian. On the other hand, such a weight vector induces a regular subdivision of the (3,8)-hypersimplex intro matroidal cells. Hence, we use information from such a subdivision to study properties of the corresponding initial degeneration. In particular, we use polyhedral geometry, commutative algebra, and computational techniques to show that all initial degenerations are smooth and, outside a single symmetry class, irreducible. This is joint work with Daniel Corey.

Dante Luber, Dan Corey
TU Berlin
luber@math.tu-berlin.de, corey@math.tu-berlin.de

MS12

Tropical Twisted Hurwitz Numbers

Tropical geometry is a successful tool for the study of structural properties of Hurwitz numbers. We review the story of tropical Hurwitz numbers before turning to a new variant which has shown up recently in the context of coverings of not necessarily oriented surfaces: twisted Hurwitz numbers. With tropical techniques, structural results like piecewise polynomiality for twisted double Hurwitz numbers can be shown. This is joint work with Marvin Hahn.

Hannah Markwig
Eberhard Karls Universität, Tübingen, Germany
hannah@math.uni-tuebingen.de

Marvin Hahn
Trinity College Dubli, Ireland
hahnma@tcd.ie

MS12

Linear Tropical Geometry with Matroids

There are several ways of computing the degree of varieties, but the most basic one is to intersect your variety with a line. We will be doing the same in the tropical world. In this talk, we will introduce the Bergman fan of a matroid, our tropical variety of interest. We study its combinatorics and identify its degree. Interesting things arise when we apply the Cremona map to the Bergman fan, which flips $x \to -x$. This new fan recovers some interesting beta invariants with the number of so called nbc bases. With the techniques developed we will compute the likelihood degeneracy degree of a matroid and recover a result from Agostini et al. All these results are algorithmic, which is a new way of computing this degree.

Raúl Penaguião
MPI MiS Leipzig
raul.penaguiao@mis.mpg.de

Federico Ardila
San Francisco State University
federico@math.sfsu.edu

Christopher Eur
Harvard University
ceur@g.harvard.edu

MS12

Linear Degenerate Tropical Flag Matroids

Grassmannians and flag varieties are important moduli spaces in algebraic geometry. Their linear degenerations arise in representation theory as they describe quiver representations and their irreducible modules. As linear degenerations of flag varieties are difficult to analyze algebraically, we describe them in a combinatorial setting and further investigate their tropical counterparts. In this talk, I will introduce matroidal, polyhedral and tropical analogs and descriptions of linear degenerate flags and their varieties obtained in joint work in progress with Alessio Borz. To this end, we introduce and study morphisms of valuated matroids. Using techniques from matroid theory, polyhedral geometry and linear tropical geometry, we use the correspondences between the different descriptions to gain insight on the structure of linear degeneration. Further, we analyze the structure of linear degenerate flag varieties in all three settings, and provide some cover relations on the poset of degenerations. For small examples, we relate the observations on cover relations to the flat irreducible locus studied in representation theory.

Victoria Schleis
Eberhard Karls Universitaet Tuebingen
victoria.schleis@student.uni-tuebingen.de

Alessio Borzi
University of Warwick
alessio.borzi@warwick.ac.uk

MS13

Khovanskii Bases for Semimixed Systems of Polynomial Equations

In this talk, I will present an efficient approach for counting roots of polynomial systems, where each polynomial is a general linear combination of fixed, prescribed polynomials. Our tools primarily rely on the theory of Khovanskii bases, combined with toric geometry, the BKK theorem, and fiber products. I will demonstrate the application of this approach to the problem of counting the number of approximate stationary states for coupled Duffing oscillators. We have derived a Khovanskii basis for the corresponding polynomial system and determined the number of its complex solutions for an arbitrary degree of nonlinearity in the Duffing equation and an arbitrary number of oscillators. This is the joint work with Paul Breiding, Mateusz Michalek, Javier del Pino and Oded Zilberberg.

Viktoriia Borovik
Osnabrück University
viktoriia.borovik@uni-osnabrueck.de

Paul Breiding
University Osnabrück
Germany
pbreiding@uni-osnabrueck.de

Javier del Pino
ETH Zürich
jdelpino@phys.ethz.ch

Mateusz Michalek, Oded Zilberberg
University of Konstanz
mateusz.michalek@uni-konstanz.de, oded.zilberberg@uni-konstanz.de

MS13

Algorithmic Confirmation of Mori Dream Spaces

Mori dream spaces (MDS) are desirable spaces to have, as they behave well with the minimal model program. However, no complete classification of Mori dream spaces yet exists. One certificate for having an MDS is to compute its Cox ring and confirm finite generation. We approach the MDS classification problem for a class of spaces called projectivized toric vector bundles (TVB) and present an algorithm, given combinatorial data related to the TVB, that produces a presentation of the corresponding Cox ring.

Courtney George, Christopher Manon
University of Kentucky
courtney.george@uky.edu, chris.manon@gmail.com

MS13

Saturation of Subalgebras, SAGBI Bases, and U-Invariants

The purpose of my talk is to present a paper (joint with A.M. Bigatti) concerning computations of subalgebras of the polynomial ring. The motivation comes from classical results about invariants of the group of unipotent matrices. A work of H.P. Kraft and C. Procesi shows that this computation can be done in a way which inspired us to introduce and study saturations of subalgebras. In the talk the merits and the limitations of our method will be shown. A particular emphasis will be given to the use of SAGBI bases. All computations were performed using original implementations by A.M. Bigatti in CoCoA 5.

Lorenzo Robbiano
University of Genoa
lorobbiano@gmail.com

MS14

Isogeny Graphs With Level Structure (Part 1)

A familiar object in isogeny based cryptography is the graph whose vertices are supersingular elliptic curves and whose edges are isogenies of fixed degree l. It is immediate to prove that from each vertex there are exactly l+1 outgoing edges, while it is less obvious that such a graph is connected and that it has the Ramanujan property, a property about the spectrum of the adjacency matrix that implies that random walks very soon visit all vertices with the same probability. In our talk we look at a generalization of these graphs, namely graphs whose vertices are pairs (E,T), where E is a supersingular elliptic curve and T is some information on the n-torsion of E (e.g. a basis, a point, a subgroup) for fixed n. It is easy to notice that the secret keys in SIDH are exactly walks in such generalized isogeny graph, and the public keys are vertices. These graphs can be multipartite, implying that the Ramanujan property is not always satisfied. By studying modular curves over mixed characteristic we relate isogeny graphs to geometric and cohomological objects, which allows us to prove the appropriate modification of the Ramanujan property. The properties of these generalized isogeny graphs are useful for a statistical zero knowledge proof of knowledge of an isogeny, which is part of a work with Basso, Connolly, De Feo, Fouotsa, Morrison, Panny, Patranabis and Wesolowski to generate elliptic curves with unknown endomorphisms.

Giulio Codogni
Università di Roma Tor Vergata
codogni@mat.uniroma2.it

MS14

Isogeny Graphs With Level Structure (Part 2)

A familiar object in isogeny based cryptography is the graph whose vertices are supersingular elliptic curves and whose edges are isogenies of fixed degree l. It is immediate to prove that from each vertex there are exactly l+1 outgoing edges, while it is less obvious that such a graph is connected and that it has the Ramanujan property, a property about the spectrum of the adjacency matrix that implies that random walks very soon visit all vertices with the same probability. In our talk we look at a generalization of these graphs, namely graphs whose vertices are pairs (E,T), where E is a supersingular elliptic curve and T is some information on the n-torsion of E (e.g. a basis, a point, a subgroup) for fixed n. It is easy to notice that the secret keys in SIDH are exactly walks in such generalized isogeny graph, and the public keys are vertices. These graphs can be multipartite, implying that the Ramanujan property is not always satisfied. By studying modular curves over mixed characteristic we relate isogeny graphs to geometric and cohomological objects, which allows us to prove the appropriate modification of the Ramanujan property. The properties of these generalized isogeny graphs are useful for a statistical zero knowledge proof of knowledge of an isogeny, which is part of a work with Basso, Connolly, De Feo, Fouotsa, Morrison, Panny, Patranabis and Wesolowski to generate elliptic curves with unknown endomorphisms.

Guido Maria Lido
Università di Roma Tor Vergata

guidomaria.lido@gmail.com

MS14

Multivariate Signature Schemes and Cryptanalysis of Early Proposals

The difficulty of solving multivariate polynomial systems makes them an interesting candidate for post-quantum cryptography. Several signature schemes have been proposed since the nineties, and although they suffer from relatively large public keys, they yield rather small signature sizes in comparison to lattice-based contributions and competitive runtimes. As is the case for most cryptographic constructions, the polynomial systems encountered in cryptographic applications are not generic: this led to the cryptanalysis of several early proposals, in particular by Kipnis and Shamir on Oil and Vinegar, which is a special case of Unbalanced Oil and Vinegar (UOV). More recently, NIST round 3 candidates GeMSS and Rainbow turned out to be much less secure than expected, with a key recovery in the case of Rainbow. Yet UOV is still standing after two decades, despite the introduction of various attacks, such as the intersection attack of W. Beullens, the Kipnis-Shamir attack and the reconciliation attack. We design a new preprocessing for MinRank before application of Grbner Bases algorithms, which allows us to obtain an original formulation of the Kipnis-Shamir attack on OV. We study the relevance of this approach to other post-quantum schemes, in particular multivariate and rank-metric.

Pierre Pébereau
LIP6
pierre.pebereau@lip6.fr

MS14

Algebraic Algorithms for Equivalence Problems

In the past few years, there has been an increased interest in hard equivalence problems. On a high level, such a problem can be defined as follows: Given two algebraic objects, find, if any, an equivalence that maps one object into the other. Several instantiations have been considered for cryptographic purposes, for example - Isomorphism of polynomials (Pattarin '96), Code equivalence (Biasse et al. '20), Matrix Code equivalence (Chou et al. '22), Alternating trilinear form equivalence (Tang et al.'22), Lattice isomorphism (Ducas & van Woerden '22). All of these problems are believed to be hard even for quantum adversaries. Conveniently, they can generically be used to build a Sigma protocol and further a post-quantum secure signature using the Fiat-Shamir transform. However, their practical hardness is still not well understood, and most of the initially proposed parameters for signature schemes have been broken. In this talk, I will focus on algebraic attacks that target several of these problems. While an equivalence problem can be inherently modeled as a system of equations, the straightforward approach is not very efficient. Turns out, there exists better modeling that allows for a significantly faster algorithm. I will show the implications of this model on the above problems and the differences arising from the particularities of the problem. For example, the presented algorithm can be used to break the proposed parameters of the signature scheme of Tang et al.'22.

Simona Samardjiska
Radboud University
simonas@cs.ru.nl

MS15

On Codes Defined over the Extended Norm-Trace Curve

In this talk we would like to introduce the class of decreasing monomial codes defined over the points of the extended norm-trace curve. We will present results on the parameters of these codes, information on the dual codes, and use this class to determine a repair scheme that repairs a single erasure with higher rates than the AG codes over the norm-trace curve. This is based on a joint work with Hiram Lopez and Gretchen Matthews.

Cícero Carvalho
Universidade Federal de Uberlândia
Uberlândia, MG - Brazil
cicero@ufu.br

MS15

Stabilizer Quantum Codes Given by Trace-Depending Polynomials

In this talk, we provide self-orthogonal evaluation codes with respect to Hermitian inner product which will give rise to good stabilizer quantum codes. In a previous paper, we proved that, considering classical codes over the finite field $\mathbb{F}_{q^{2n}}$, obtained by evaluating at the roots of the trace polynomial of $\mathbb{F}_{q^{2n}}$ with respect to $\mathbb{F}_q$, one gets q^{2n}-ary codes whose q^2-ary subfield-subcodes give rise to excellent q-ary quantum codes. A main inconvenient of the above codes is that they offer few options with respect to their lengths. Therefore, we propose to evaluate at the roots of *trace-depending polynomials* which we will define in the talk. This procedure provides a wider range of lengths although to prove self-orthogonality is harder. We show their advantages by giving a table of quantum records with respect to M. Grassl table. The above records are obtained by computation and a complete theoretical study is very difficult. In the talk, we detail the study we performed in [Stabilizer quantum codes defined by trace-depending polynomials. Finite Fields Appl. 87 (2023)] of codes obtained by evaluating at the roots of a specific class of trace-depending polynomials. This study gives rise to very good quantum codes derived of Hermitian self-orthogonal subfield-subcodes of codes of the above class. This is a joint work with Hernando, Martn-Cruz and Ruano.

Carlos Galindo, Fernando Hernando, Helena Martín-Cruz
University Jaume I
galindo@mat.uji.es, carrillf@uji.es, martinh@uji.es

Diego Ruano
IMUVA-Mathematics Research Institute
University of Valladolid, Spain
diego.ruano@uva.es

MS15

Linear Codes Associated to Determinantal Varieties

We give the complete weight distribution of determinantal codes, which are linear codes associated to projective algebraic varieties defined by the vanishing of minors of a fixed size of a generic matrix. Further, we consider variants of these linear codes that are called open determinantal codes, and observe that they generalize known constructions of linear codes associated to general linear groups over finite fields. The weight distribution and the minimum distance of these open determinantal codes is also determined. In the process, we prove in the affirmative a three-part conjecture of Beelen and Ghorpade. Connections of these results to several parts of discrete mathematics will also be outlined.

Sudhir Ghorpade
Indian Institute of Technology Bombay
srg@math.iitb.ac.in

Mahir Bilen Can
Tulane University, New Orleans, Louisiana, USA
mcan@tulane.edu

MS15

Weights of Evaluation Codes

In this talk, we show several formulas for the length, dimension, minimum distance and generalized Hamming weights of evaluation codes. These formulas are in terms of the Hilbert-Samuel multiplicity and in the number of points of certain finite varieties. In particular, we give formulas for the generalized Hamming weights of Reed-Muller-type codes, Toric codes over hypersimpleces and squarefree evaluation codes. We present some examples of how to compute these formulas over an affine curve.

Delio Jaramillo-Velez
CINVESTAV
delin.jaramillo@gmail.com

MS16

Network Decoding, Part II

The one-shot capacity of an adversarial multicast network gives a measure of how many alphabet symbols can be sent reliably through the network during a single transmission round. In this talk, we show that in the scenario where the adversary's action is confined to a proper subset of network edges, traditional cut-set bounds are not tight, and that their non-sharpness comes precisely from restricting the action of the adversary. We will discuss the necessity of non-linear functions (e.g. decoding or authentication) at intermediate network nodes when an adversary is restricted, as well as improved bounds on one-shot capacity in this setting.

Allison Beemer
University of Wisconsin, Eau Claire
beemera@uwec.edu

Altan Kilic, Alberto Ravagnani
Eindhoven University of Technology
a.b.kilic@tue.nl, a.ravagnani@tue.nl

MS16

Network Coding Meets Crypto

In this talk, we show how information-theoretic security can be combined with any cryptosystem to obtain a hybrid universal network-coding cryptosystem (HUNCC). To achieve this, we employ a secure network coding scheme to premix the data, followed by encrypting a small portion of the mixed data before transmitting it across an untrusted network. By encrypting only a small fraction of the mixed messages, HUNCC is able to amortize the various costs associated with encryption, including communication throughput, energy consumption, and computational time complexity, while still providing strong and provable security guarantees.

Rafael D'Oliveira
Clemson University
rdolive@clemson.edu

MS16

Network Decoding, Part I

This talk focuses on the (one-shot) capacity of multicast networks, which measures the maximum number of alphabet symbols that can be sent error-free in a single transmission round. This talk will consist of two parts. In the first part, we recover and extend various results on the capacity of a single-source multi-terminal noiseless network over small alphabet sizes using solely a mixed integer programming approach. In the second part of the talk, we focus on adversarial networks with an adversary who can possibly corrupt only a proper subset of network edges. We show that linear network coding does not suffice to achieve capacity unlike the classical network coding setting (implying a need for decoding in the intermediate vertices of the network). We conclude by showing some indications that the optimization approach introduced in the first part of the talk can be beneficial for adversarial networks introduced in the second part of the talk, as well. The new results in this talk are based on joint work with A. Beemer and A. Ravagnani and on joint work with C. Hojny and A. Ravagnani.

Altan Kilic
Eindhoven University of Technology
a.b.kilic@tue.nl

MS16

Rank Metric Codes for Security and Reliability of Network and Storage Systems

Rank metric codes have attracted significant interest from the research community due to their potential to improve the reliability and security of networking and storage systems. Rank metric codes enable the networks to transmit information in the presence of malicious links and nodes that can inject errors in different parts of the network. In storage systems, rank-metric codes enable fast recovery from a broad range of error and erasure patterns, including crisscross errors. We will begin with a quick overview of rank-metric codes and their contractions and related bounds. Next, we will survey the application of rank metric codes for network error correction and secure network coding. Next, we will focus on the notion of locality in the rank and subspace metrics. In particular, we will present a class of locally repairable array codes in the rank metric. We also derive a Singleton-like upper bound on the minimum rank distance of (linear) codes with 'rank-locality' constraints. Our proposed construction achieves this bound for a broad range of parameters. Finally, we construct a class of constant-dimension subspace codes (also known as Grassmannian codes) with locality constraints in the subspace metric.

Alex Sprintson
Texas A&M University

spalex@ece.tamu.edu

MS17

The Cone of Nonnegative Forms on Genus One Curves

The study and characterization of non-negativity for polynomials (or forms) dates back to D. Hilbert, whose classical result characterize the number of variables and the degrees for which non-negative forms on $\mathbb{P}^n$ coincide with sums of squares. In the last decades, the relation between non-negativity and sums of squares received increasing attention, in connection with convex geometry: the work of Hilbert has been recently extended by G. Blekherman, R. Sinn, G. Smith and M. Velasco, that consider the cones of non-negative and sums of squares forms on projective varieties. In this talk, we consider the cones P_C of non-negative quadratic forms on projective curves $C \subset \mathbb{P}^n$. When C is a rational normal curve, the extremal rays and the faces of P_C can be deduced from the case of $\mathbb{P}^1$. On the other hand, very little is know in general. We start describing the relation between the faces of P_C and effective divisord on C, and then we focus on genus one curves, in particular plane cubic curves $C \subset \mathbb{P}^2$. Using the group law on C, we describe the extremal rays and the faces of P_C, providing explicit Krivine-Stengle-type certificates of non-negativity. We conclude generalizing this description, from quadratic form on plane cubics to even degree forms on elliptic normal curves.

Lorenzo Baldi
Sorbonne Université, CNRS
PolSys - Polynomial Systems LIP6, Paris, France
lorenzo.baldi@inria.fr

Greg Blekherman
Georgia Institute of Technology
gblekherman3@gatech.edu

Rainer Sinn
University of Leipzig
rainer.sinn@uni-leipzig.de

MS17

Convex Hulls of Monomial Curves, and a Sparse Positivstellensatz

Most of what I will speak about is joint work with Gennadiy Averkov. Let $C \subseteq \mathbb{R}^n$ be a semialgebraic curve, let K be its closed convex hull. We show that K admits a lifted semidefinite description by finitely many linear matrix inequalities (LMIs), each of size $k := \lfloor \frac{n}{2} \rfloor + 1$. Although the proof is non-constructive in general, it becomes entirely constructive when C is a monomial curve, given parametrically as $(t^{m_1}, \ldots, t^{m_n})$ with t varying in an interval. In this case, K is described by $\mathcal{O}(d)$ LMIs of size k, where $d = \max\{m_1, \ldots, m_n\}$ is the degree of the curve. On the dual side we prove that if a univariate polynomial $p(t)$ of degree d with at most $2k+1$ monomials is non-negative on $\mathbb{R}_+$, then p admits a representation $p = t^0\sigma_0 + \cdots + t^{d-k}\sigma_{d-k}$ where the polynomials σ_i are sums of squares and $\deg(\sigma_i) \leq 2k$. The latter is a sparse positivstellensatz for univariate polynomials. Our results fit into the general attempt of formulating polynomial optimization problems as semidefinite problems with LMIs of small size.

Claus Scheiderer
Univ Konstanz (Germany)
claus.scheiderer@uni-konstanz.de

MS17

Positivity and Its Non-Reduced Structures

Cones of non-negative polynomials are usually studied in the context of homogeneous polynomials as one obtains convex cones in finite-dimensional vector spaces. However, if one considers the cone without any degree bound, one observes that faces, whose linear span is an ideal, play a special role. I will describe the corresponding (saturated, homogeneous) ideal in the homogeneous setting.

Christoph Schulze
TU Dresden
christoph.schulze3@tu-dresden.de

MS17

Sums of Squares on Surfaces

How do we effectively verify that a polynomial function is nonnegative? We will certify nonnegativity by exhibiting a nonnegative multiplier such that the product is a sum of squares. Unexpectedly, our techniques are particularly well-suited to produce new bounds on the degrees of nonnegative functions on rational surfaces. This talk is based on joint work with Grigoriy Blekherman, Rainer Sinn, and Mauricio Velasco.

Gregory G. Smith
Queen's University
ggsmith@mast.queensu.ca

MS18

Minimal Sparsity for Scalable Moment-Sos Relaxations of the Ac-Opf Problem

AC-OPF (Alternative Current - Optimal Power Flow) aims at minimizing the operating costs of an AC power grid. It is well-known to be a difficult optimization problem in general, as it reformulates as a nonconvex QCQP (Quadratically Constrained Quadratic Program). The moment-SOS (Sums-Of-Squares) hierarchy has proved relevant to solve AC-OPF instances to global optimality. However, obtaining the convergence of the hierarchy may requires to go beyond the first step of the involved sequence of SDP (Semidefinite Programming) relaxations, and thus to solve semidefinite programs whose size grows drastically at each step of the hierarchy. Thus, the application of such relaxations to large scale AC-OPF problems (with more than 10 000 variables) remains a challenging computing task. Large polynomial optimization problems can be tackled efficiently if they are sufficiently sparse. Exploiting the new framework of correlative-term sparsity, it is now possible to compute partial second order moment relaxations for large scale power grids. In this talk, we present a new sparsity pattern, that we call minimal sparsity, inspired by the specific structure of the AC-OPF problem. We show that minimal sparsity enables the computation of second order moment-SOS relaxations on instances with tens of thousands of variables. Experimentally, we observe that it also provides tighter lower bounds to certify the global optimality of AC-OPF solutions.

Victor Magron
CNRS LAAS
victor.magron@laas.fr

Adrien Le Franc
LAAS CNRS
adlefranc@laas.fr

MS18

Frequency-Domain Methods and Polynomial Optimization in Structural Engineering

Let us consider the problem of the design of a structure, such as a bridge, an aircraft wing, or bicycle frame. In structural engineering, one wishes to optimize an objective such as minimum compliance in the parameters of the structure, such as the areas of element cross-sections, such that it withstands given loads. M. Tyburec, J. Zeman, M. Kruzik, D. Henrion [Global optimality in minimum compliance topology optimization of frames and shells by moment-sum-of-squares hierarchy. Structural and Multidisciplinary Optimization 64(4):1963-1981, 2021.] have recently considered the case when the loads are time-invariant. We show how to approach the case when the loads are time-varying, with a finite number of harmonics.

Shenyuan Ma, Saman Khorramian, Marek Tyburec,
Vyacheslav Kungurtsev, Jakub Marecek
Czech Technical University
shenyma@fel.cvut.cz, khorrsam@fel.cvut.cz,
marek.tyburec@cvut.cz, kunguvya@fel.cvut.cz,
jakub.marecek@fel.cvut.cz

MS18

Using the Christoffel Darboux Kernel for the Estimation of Discontinuous Function: Application to Parametrized Conservation Laws

This talk is about the numerical computation of solutions to parametrized conservation laws. After a brief presentation of the Lasserre's hierarchy, we will explain how it can be applied in the context of parametrized conservation laws, that is a difficult task in general due to the underlying discontinuity of the solutions. The general idea of the Lasserre's hierarchy is to obtain generalized moments of the parametrized conservations. Then, we show how to obtain the solution itself through the use of the Christoffel-Darboux kernel. This is a joint work with Anthony Nouy, Clment Cardon, and Nicolas Seguin.

Swann Marx
LS2N-CNRS, Nantes
swann.marx@ls2n.fr

MS18

Moment-SoS Methods for Some Optimal Transport Problems

Most optimal transport (OT) solvers are currently based on an approximation of underlying measures by discrete measures. Another route is to approximate moments of measures, when these are determinate. Here, we show that many common OT problems can be formulated as generalized moment problems. These include the computation of Lp Wasserstein or Gromov-Wasserstein distances and the corresponding barycenters. For measures supported on compact semi-algebraic sets, a practical numerical approach then consists in truncating moment sequences up to a certain order, and using the polynomial sums-of-squares hierarchy. The approach is proved to converge. It allows to extract a posteriori relevant information on the measures, such as their supports that can be estimated using Christoffel-Darboux kernels. We finally discuss how this approach could be made computationally feasible by the use of low-rank tensor methods. This is a joint work with Olga Mula. Reference: [1] O. Mula and A. Nouy. Moment-SoS methods for optimal transport problems, arXiv:2211.10742, 2022.

Anthony Nouy
Ecole Centrale Nantes
anthony.nouy@ec-nantes.fr

MS19

Structural Identifiability of Series-Parallel LCR Systems

In this talk, we consider the structural identifiability problem for the parameters of series-parallel LCR circuit networks. We first investigate networks with only two classes of components (inductor-capacitor (LC), inductor-resistor (LR), and capacitor-resistor (RC)), and conclude that local identifiability can be determined by only comparing the number of base elements in the system and coefficients in the defining constitutive equation. We then investigate the general series-parallel LCR circuits (with all three classes of components), exploring possible methods for classifying identifiability and examining key examples which exhibit why the general LCR case will require novel techniques in further study.

Cashous Bortner
California State University, Stanislaus
cbortner@csustan.edu

Seth Sullivant
North Carolina State University
smsulli2@ncsu.edu

MS19

Identifiability and the Singular Locus of Certain Linear Compartmental Models

A linear compartmental model is identifiable when its parameters can be recovered from data. Given a linear compartmental model, we want to use its inputs, outputs, and leaks to determine its identifiability. We focus on two types of models: a model whose underlying graph is a directed cycle, and catenary models, whose underlying graph is a bidirected path. For directed cycles, we discuss how the number and placement of leaks can prevent identifiability and present some factors of the equation of the singular locus for identifiable models. For catenary models, we provide an expression of the coefficients of the input-output equations using symmetric functions. Finally, we explore if reducing directed cycle models by removing compartments preserves the identifiability of the model.

Natasha Crepeau
University of Washington
ncrepeau@uw.edu

MS19

Structural and Practical Identifiability of ERK Kinetics

This talk is based on a paper written in collaboration with Lewis Marsh, Helen Byrne and Heather Harrington, where we explored the algebra, geometry and topology of ERK kinetics. The MEK/ERK signalling pathway is involved in cell division, cell specialisation, survival and cell death. We studied a polynomial dynamical system describing the dynamics of MEK/ERK proposed by Yeung et al. with their experimental setup, data and known biological information. The experimental dataset is a time-course of ERK measurements in different phosphorylation states following activation of either wild-type MEK or MEK mutations associated with cancer or developmental defects. My focus in this talk will be on identifiability, both structural and practical. Structurally identifiable is concerned with asking whether parameter values can be recovered from perfect data. Practical identifiability addresses the more realistic situation where we assume there is measurement noise. We observe that the original model is structurally but not practically identifiable. We will discuss how algebraic quasi-steady state approximation leads to a smaller simpler model which is both structurally and practically identifiable, while providing a probable explanation for the practical non-identifiability of the original model.

Lewis Marsh
Mathematical Institute, University of Oxford
marsh@maths.ox.ac.uk

Emilie Dufresne
University of York
emilie.dufresne@york.ac.uk

Helen M. Byrne, Heather Harrington
Mathematical Institute
University of Oxford
helen.byrne@maths.ox.ac.uk, harrington@maths.ox.ac.uk

MS19

How Often Do We Encounter Locally-But-Not-Globally-Identifiable Parameters in Systems Biology, and Why?

Structural identifiability determines the possibility of estimating the parameters of a model by observing its output in an ideal experiment. If a parameter is structurally globally identifiable, its true value can be uniquely inferred. If it is structurally locally but not globally identifiable (SLNGI), it is uniquely determined in a neighbourhood of its nominal value, but at least one distant value exists which yields an identical output. In the systems biology literature it has been suggested that local identifiability usually entails global identifiability. If true, this would mean that local identifiability tests (which are easier than global ones) are sufficient for most practical applications. Although counter-examples have been found, this assumption has never been thoroughly investigated. To clarify this matter, we first approach it empirically by analysing 102 models with a total of 763 parameters. We obtain that approximately 5% of the parameters are SLNGI. Next, we explain the SLNGI parameters as a result of particular features of the model equations, and we calculate the equivalent solutions numerically. We find that in some cases the equivalent solutions involve negative parameters and/or initial conditions, which do not make sense biologically. Our results suggest that in most systems biology applications it is indeed sufficient to ensure structural local identifiability, since the spurious solutions cannot be mistaken for the real one.

Xabier Rey Barreiro
Universidade de Vigo
Department of Systems Engineering and Control
xabier.rey@uvigo.gal

Alejandro F. Villaverde
Universidade de Vigo
CITMAga
afvillaverde@uvigo.gal

MS20

Rational Partition Models Under Iterative Proportional Scaling

The classical iterative proportional scaling algorithm, or IPS, numerically computes the maximum likelihood estimate of a given vector of counts for a log-linear partition model. We investigate the conditions under which IPS produces the exact maximum likelihood estimate, or MLE, in finitely many steps. Since IPS produces a rational function at each step, a necessary condition is that the model must have rational maximum likelihood estimator. However, the convergence is highly parametrization-dependent; indeed, one parametrization of a model may exhibit exact convergence in finitely many steps while another does not. We introduce the generalized running intersection property, which guarantees exact convergence of IPS. As the name suggests, this strictly generalizes the well-known running intersection property for hierarchical models. This generalized running intersection property can be understood in terms of the toric geometry of the log-linear model, and models that satisfy this property can be obtained by performing repeated toric fiber products of linear ideals. We also draw connections between models that satisfy the generalized running intersection property and balanced, stratified staged trees.

Jane Coons
St John's College, University of Oxford
jane.coons@sjc.ox.ac.uk

Carlotta Langer
University of Hamburg
carlotta.langer@web.de

Michael G. Ruddy
University of San Francisco
mruddy@usfca.edu

MS20

Optimisation in Polyhedral Norms

Given a set, X, of points in space, $\mathbb{R}^n$, and a metric, a Voronoi diagram partitions $\mathbb{R}^n$ into the regions by identifying all the points closer to a fixed point in the set with respect to the given metric. The region corresponding to that point is called its Voronoi cell. Set of points in the space whose distance to X is optimised by (at least)two different points in X define its medial axis. In this talk I will present results on Voronoi cells of codimension-one varieties with respect to polyhedral norm. In particular, I will discuss description and computations of the medial axis. This is based on the joint work with Duarte, Lindberg, Torres, and Weinstein.

Eliana Duarte
Centro de Matematica Universidade do Porto
Max-Planck-Institute for Mathematics in the Scinces
eliana.gelvez@fc.up.pt

Nidhi Kaihnsa
Brown University, Providence,Rhode Island
nidhi@math.ku.dk

Julia Lindberg
University of Wisconsin-Madison, USA
jrlindberg@wisc.edu

Angelica Torres
Centre de Recerca Matemàtica
atorres@crm.cat

Madeleine Weinstein
University of Puget Sound
mweinste@stanford.edu

MS20

Symmetries in Directed Gaussian Graphical Models

Gaussian graphical models have manifold applications in statistics. Vertex and edge symmetries appear in various applications and it is desirable to capture these symmetries in the model itself. For this, we define Gaussian graphical models on directed acyclic graphs (DAGs) with coloured vertices and edges, calling them restricted DAG (RDAG) models. If two vertices or edges have the same colour, their parameters in the model must be the same. Thus, RDAG models are a natural directed analogue of (undirected) RCON models, see [Hjsgaard and Lauritzen, Graphical Gaussian models with edge and vertex symmetries, J. R. Stat. Soc. Ser. B Stat. Methodol., 70(5):1005-1027, 2008]. In this talk, we characterize maximum likelihood (ML) estimation of RDAG models. Using properties of the underlying DAG and its colouring we give bounds on ML thresholds, which show that symmetries decrease thresholds. Moreover, we characterize when an RDAG model is equal to its induced RCON model, which allows to study these RCON models via RDAG models.

Visu Makam
University of Melbourne, Australia
visu.makam@unimelb.edu.au

Philipp Reichenbach
TU Berlin
reichenbach@tu-berlin.de

Anna Seigal
Harvard University, U.S.
aseigal@seas.harvard.edu

MS20

Voronoi Cells and Maximum Likelihood Estimation

Given a matrix M in a linear concentration model, the set of covariance matrices of observed data for which M is the maximum likelihood estimate forms a spectrahedron known as the logarithmic Voronoi spectrahedron. We study how the logarithmic Voronoi spectrahedra vary over a linear concentration model.

Madeleine Weinstein
University of Puget Sound
mweinste@stanford.edu

Yulia Alexandr
UC Berkeley
yalexandr@berkeley.edu

Margaret H. Regan
Duke University
Durham, NC USA
mregan@math.duke.edu

MS21

Restricted Secants of Grassmannians

Restricted secant varieties of Grassmannians are constructed from sums of points corresponding to k-planes with the restriction that their intersection has a prescribed dimension. We study dimensions of restricted secant of Grassmannians and relate them to the analogous question for secants of Grassmannians via an incidence variety construction. We define a notion of expected dimension and give a formula for the dimension of all restricted secant varieties of Grassmannians that holds if the BDdG conjecture on non-defectivity of Grassmannians is true. We also demonstrate example calculations in Macaulay 2, and point out ways to make these calculations more efficient. We also show a potential application to coding theory.

Dalton Bidleman, Luke Oeding
Auburn University
deb0036@auburn.edu, oeding@auburn.edu

MS21

The Average Condition Number of Most Tensor Rank Decomposition Problems is Infinite

The condition number of the tensor rank decomposition measures the sensitivity of the rank-1 summands with respect to perturbations. We show for random rank-2 tensors that the expected value of the condition number is infinite for a wide range of choices of the density. Under a mild additional assumption, we show that the same is true for most higher ranks $r \geq 3$ as well. In fact, as the dimensions of the tensor tend to infinity, asymptotically all ranks are covered by our analysis. Our results underline the high computational complexity of computing tensor rank decompositions.

Paul Breiding
University Osnabrück
Germany
pbreiding@uni-osnabrueck.de

Carlos Beltran
Universidad de Cantabria
carlos.beltran@unican.es

Nick Vannieuwenhoven
Departement Computerwetenschappen
KU Leuven
nick.vannieuwenhoven@kuleuven.be

MS21

Reciprocal Variety of Tensors and Stratification of Tensor Spaces

The so-called reciprocal variety of a 1_A-generic cubic tensor is the image of its first flattening under the birational map reversing matrices. In this talk, we will address the study of the invariants of this rational variety, starting with the initial case of the pencil of matrices. This approach naturally leads to new stratification of tensor spaces, and we present some of these stratifications.

Hanieh Keneshlou
University of Konstanz

hanieh.keneshlou@uni-konstanz.de

MS21

Identifiability of Sum of Squares

Although the decomposition of a polynomial as sums of squares is not unique due to the natural action of the orthogonal group, we may still ask if the decomposition is unique up to this action. In this talk, I will discuss the results of a joint work with Andrew Ferguson, Giorgio Ottaviani and Mohab Safey El Din and an in-progress work with Giorgio Ottaviani.

Ettore Teixeira Turatti
UiT The Arctic University of Norway
ettore.t.turatti@uit.no

MS22

Sequential Learning with Hankelized Tensor Factorization for Next Item Recommendations

Self-attentive transformer models have recently been shown to solve the next item recommendation task very efficiently. The learned attention weights capture sequential dynamics in user behavior and generalize well. Motivated by the special structure of learned parameter space, we question if it is possible to mimic it with an alternative and more lightweight approach. We develop a new tensor factorization-based model that ingrains the structural knowledge about sequential data within the learning process. We demonstrate how certain properties of a self-attention network can be reproduced with our approach based on special Hankel matrix representation. The resulting model has a shallow linear architecture. Remarkably, it achieves significant speedups in training time over its neural counterpart and performs competitively in terms of the quality of recommendations.

Evgeny Frolov, Ivan Oseledets
Skolkovo Institute of Science and Technology
evgeny.frolov@skoltech.ru, ivan.oseledets@gmail.com

MS22

Complete Decomposition of Symmetric Tensors in Linear Time and Polylogarithmic Precision

We study symmetric tensor decompositions, i.e. decompositions of the input symmetric tensor T of order 3 as sum of r 3rd-order tensor powers of u_i where u_i are vectors in $\mathbb{C}^n$. In order to obtain efficient decomposition algorithms, it is necessary to require additional properties from the u_i. In this paper we assume that the u_i are linearly independent. This implies that r is at most n, i.e., the decomposition of T is undercomplete. We will moreover assume that $r = n$ (we plan to extend this work to the case where r is strictly less than n in a forthcoming paper). We give a randomized algorithm for the following problem: given T, an accuracy parameter epsilon, and an upper bound B on the condition number of the tensor, output vectors u'_i such that u_i and u'_i differ by at most epsilon (in the l_2 norm and up to permutation and multiplication by phases) with high probability. The main novel features of our algorithm are: (1) We provide the first algorithm for this problem that works in the computation model of finite arithmetic and requires only poly-logarithmic (in n, B and $1/\varepsilon$) many bits of precision. (2) Moreover, this is also the first algorithm that runs in linear time in the size of the input tensor. It requires $O(n^3)$ arithmetic operations for all accuracy parameters $\varepsilon = 1/\text{poly}(n)$. Joint work with Pascal Koiran and the preprint is available at (https://arxiv.org/abs/2211.07407)

Pascal Koiran, Subhayan Saha
LIP, ENS Lyon
pascal.koiran@ens-lyon.fr, subhayansaha14@gmail.com

MS22

The Barycenter in Free Nilpotent Lie Groups and Its Application to Iterated-Integrals Signature Tensors

Iterated-integrals signature (IIS) is a powerful tool to encode information about d-dimensional paths, which attracted growing interest in statistics and machine learning. IIS can be viewed as a collection of tensors of increasing order, and the truncated signature (signature tensors from order 1 to L) lives in a nilpotent free Lie group. In this contribution, we establish well-definedness of the barycenter for every integrable measure on the free nilpotent Lie group of step L (over $\mathbb{R}^d$). We show that the barycenter can be computed recursively, order by order, by a finite-time algorithm. If time permits, we will discuss an application of barycenters to averaging time series data in statistics.

Marianne Clausel
Université de Lorraine
marianne.clausel@univ-lorraine.fr

Joscha Diehl
University of Greifswald
joscha.diehl@gmail.com

Raphael Mignot
Université de Lorraine
raphael.mignot@univ-lorraine.fr

Leonard Schmitz
University of Greifswald
leonard.schmitz@uni-greifswald.de

Nozomi Sugiura
Japan Agency for Marine-Earth Science and Technology
nsugiura@jamstec.go.jp

Konstantin Usevich
CNRS and Université de Lorraine
konstantin.usevich@univ-lorraine.fr

MS22

Tensor-Based Methods for the Solution of Noisy Overdetermined Systems

Systems of polynomial equations form an essential modelling tool in engineering applications. Typical in these applications is the presence of noise, but also of additional measurements/equations to mitigate its effect. Unfortunately, most established methods to solve systems of polynomial equations are limited to square systems, making them inadequate for such applications. Square systems also have a fixed number of roots, equal to the Bézout number, which is typically more than expected from the physical interpretation of the problem. We contribute to the development of tensor-based tools to solve polynomial systems of equations, specifically in overdetermined settings. The method involves computing the nullspace of the Macaulay matrix associated with the system, from which it recovers the roots through a low-rank decomposition of a third-order tensor. In many practical cases, this method is guaranteed to retrieve all roots. Different algorithms for the low-rank decomposition are presented, especially useful in the case of noise. As a result, the method can take advantage of additional noisy equations to improve the estimates of roots. The practical utility is shown for a blind multi-source localization problem where the position of two transmitters is estimated solely on the power received at an arbitrary configuration of antennas in their vicinity.

Lieven De Lathauwer
KU Leuven
lieven.delathauwer@kuleuven.be

Raphael Widdershoven
ESAT-STADIUS
KU Leuven
raphael.widdershoven@kuleuven.be

Nithin Govindarajan
KU Leuven
nithin.govindarajan@kuleuven.be

MS23

A Symbolic-Numeric Method to Isolate Real and Complex Eigenvalues

The location of eigenvalues has been an interest for various reasons, including root finding, root certification of polynomial systems and stability region of differential equations. In this study, we describe a symbolic-numeric method, based on Hermite quadratic forms, to define a neighborhood that includes a real eigenvalue with a certain precision. Then we locate complex eigenvalues and distinguish the neighborhoods according to the signs of their real parts. We also show that these neighborhoods can define a stability region, provide a reality certification or guarantee convergence for some numerical methods.

Tülay Ayyildiz
Karadeniz Technical University
tulayayyildiz@gmail.com

MS23

On the Complexity of Chow Forms

The Chow form of a projective variety is a classical construction in algebraic geometry and its computation is particularly important in elimination theory. Recently, generalizations of this construction for multiprojective varieties have been introduced and studied. The first part of this talk will be a swift introduction to Chow forms and its relatives in the multiprojective space. In the second part of the talk, we will present an algorithm to compute the Chow form. The algorithm relies on a resultant computation. Furthermore, in the case of multiprojective varieties, the algorithm correctly makes use of the sparseness in the input by switching to sparse resultants.

Levent M. Dogan
Technische Universität Berlin
Germany
dogan@math.tu-berlin.de

MS23

A Polyhedral Description of Complex Polynomial Maps on the Plane

We say that two continuous maps $f, g : X \to Y$ are topologically equivalent if there exist homeomorphisms $\varphi : X \to X$ and $\psi : Y \to Y$ such that $\psi \circ f \circ \varphi = g$. For any positive integer d, there are finitely many topological equivalence classes of polynomial maps of degree d on the complex plane. Due to the abscence of a systematic approach, their number, denoted by $\Theta_{\mathbb{C}}(d)$, is computed only for the case where $d = 2$. The *Newton tuple* of a polynomial map is the collection of Newton polytopes corresponding to the respective polynomials of the map. It is shown that all generic maps with a fixed Newton pair contribute to the same element in $\Theta_{\mathbb{C}}(d)$. I will present results relating topological invariants of generic maps to their Newton pairs. This gives rise to a polyhedral method that produces a lower bound on $\Theta_{\mathbb{C}}(d)$ for arbitrary d. We compute the latter by implementing a software package on OSCAR. This is a joint work with Kemal Rose (MPI MIS Leipzig).

Boulos El Hilany
Technische Universität Braunschweig
b.el-hilany@tu-braunschweig.de

Kemal Rose
Max-Planck Institute for Mathematics in the Sciences
kemal.rose@mis.mpg.de

MS23

Conditioning and Stability of Fundamental Matrix Computation

This talk is to report the first step of a study on conditioning and stability of minimal solvers in computer vision. We'll clarify the basic concepts from a numerical analysispoint of view and see their implications in design and analysis of minimalsolvers for the specific case of computing the fundamental matrix. Joint work with Sameer Agarwal, Erin Connely, and Rekha Thomas.

Alperen Ergur
University of Texas, San Antonio
alperen.ergur@utsa.edu

MS24

Topology and Signatures

The path signature is a structured description of sequential data, such as multivariate time series, as an infinite sequence of tensors. This description characterizes the underlying path and provides a powerful tool to summarize time series. The path signature originated in K. T. Chen's work on iterated integrals in topology. In this talk, we discuss how this topological perspective leads to generalizations of the path signature to higher dimensional data.

Darrick Lee
University of Pennsylvania
darrick.lee@maths.ox.ac.uk

MS24

Shortest Paths in General Polyhedral Surfaces

Any surface that is intrinsically polyhedral can be represented by a collection of simple polygons (which we call fragments), glued along pairs of equally long oriented edges, where each fragment is endowed with the geodesic metric arising from its Euclidean metric. We refer to such a representation as a portalgon, and we call two portalgons equivalent if the surfaces they represent are isometric. We analyze the complexity of shortest paths. We call a fragment happy if any shortest path on the portalgon visits it at most a constant number of times. A portalgon is happy if all of its fragments are happy. We present an efficient algorithm to compute shortest paths on happy portalgons. The number of times that a shortest path visits a fragment is unbounded in general. We contrast this by showing that the intrinsic Delaunay triangulation of any polyhedral surface corresponds to a happy portalgon. Since computing the intrinsic Delaunay triangulation may be inefficient, we provide an efficient algorithm to compute happy portalgons for a restricted class of portalgons.

Maarten Loffler
Utrecht University
m.loffler@uu.nl

Tim Ophelders
TU Eindhoven
t.a.e.ophelders@uu.nl

Rodrigo Silveira
Universitat Politècnica de Catalunya
rodrigo.silveira@upc.edu

Frank Staals
Utrecht University
f.staals@uu.nl

MS24

Discretizations of the PHT; How Big Can a Minimum Faithful Set of (Augmented) Persistence Diagrams Be?

Given a geometric simplicial complex embedded in $\mathbb{R}^d$, there exist finite sets of topological descriptors generated by lower-star filtrations in various directions that, together, faithfully represent the complex, a fact that is the foundation of many recent developments in shape comparison. In this talk, we focus on better understanding the minimum cardinality of faithful sets. In particular, we construct simplicial complexes for which minimum faithful sets of topological descriptors have surprisingly high cardinality. These constructions will highlight stark practical differences between augmented (sometimes called "ephemeral') descriptors and standard, non-augmented descriptors. We present our results in terms of persistence diagrams, but highlight how we can make parallel statements for Betti curves and Euler characteristic curves.

Anna Schenfisch
Montana State University
annaschenfisch@montana.edu

Brittany Fasy
Tulane University
brittany@cs.montana.edu

Samuel Micka
Western Colorado University
smicka@western.edu

David Millman
Blocky Inc.
dave@blocky.rocks

MS24

Cofibrant Indecomposables in Chain Complex Valued Tame Functors Indexed by Dimension One Posets

In this work, we provide a model structure on full subcategories of tame objects in functor categories indexed by continuous realizations of posets of dimension 1. We also characterize the indecomposable cofibrant objects when the landing category is the one of bounded non-negative chain complexes. In addition, we present a general method to construct indecomposables in a functor category by a gluing technique.

Wojciech Chacholski
KTH
wojtek@math.kth.se

Barbara Giunti
Technische Universität Graz
bgiunti@tugraz.at

Claudia Landi
University of Modena and Reggio Emilia
claudia.landi@unimore.it

Francesca Tombari
KTH Royal Institute of Technology
tombari@kth.se

MS25

Geometric Relations on Plabic Graphs, Totally Non-Negative Grassmannians and Applications

A. Postnikov parametrized totally nonnegative Grassmannians in terms of discrete path integration on planar bicoloured graphs in the disc. An alternative parametrization was proposed by T. Lam in terms of systems of relations at the vertices of such graphs, depending on some edge signatures to compute scattering amplitudes for on-shell diagrams N=4 Super Yang Mills and govern the totally nonnegative amalgamation of the little positive Grassmannians into any given positroid cell. With P.G. Grinevich, we have provided an explicit characterization of the signatures corresponding to the totally non-negative cells and an explicit solution of the system of relations. The components of the edge vectors are rational in the edge weights with subtraction-free denominators. The combinatorial representation of the geometric signatures is a Kasteleyn-type property when the graph is also bipartite. As an application, we have constructed an explicit map from graphs representing a given irreducible positroid cell in the totally nonnegative Grassmannian to the spectral data for the class of real regular Kadomtsev-Petviashvili II (KPII) solutions establishing a bridge between real regular finite-gap KPII solutions and real regular multiline KPII solitons studied by S. Chakravarthy and Y.Kodama and by Y. Kodama and L.K. Williams. Time permitting, we will also present recent results for the generalizations of the above results to bipartite graphs in the annulus.

Simonetta Abenda
Department of Mathematics, University of Bologna and
INFN Bo
Bologna, Italy
simonetta.abenda@unibo.it

Petr Grinevich
Steklov Mathematical Institute of Russian Academy of Science
pgg@landau.ac.ru

MS25
On Degenerate Sigma Functions

We consider the class of entire functions on Jacobi varieties of plane algebraic curves called sigma functions. Such a function is presented by an analytic series in the coordinates of the corresponding Jacobi variety with coefficients polynomial in parameters of the corresponding curve. Recently, the theory of multivariable sigma functions was developed (by Buchstaber and Leykin), which provides a powerful apparatus of constructing series representations for the sigma functions of plane algebraic curves. Hirota equations and addition laws are also produced by this apparatus. As an analytic series a sigma function can be degenerated together with the corresponding curve. As an example, we obtain explicit expressions for genus 2 degenerate sigma function in terms of genus 1 sigma function and elementary functions, derive a solution of the generalized Jacobi problem on an elliptic curve, show the process of collapsing a rank 4 lattice to a rank 3 one in the case of such a degeneration.

Julia Bernatska
University of Connecticut
jbernatska@gmail.com

MS25
Computational Approach to the Schottky Problem

We present a computational finite precision approach to the classical Schotky problem whether a principally polarized Abelian variety (PPAV) is a Jacobian variety, i.e., whether a complex symmetric matrix with positive-definite imaginary part is the matrix of periods of a Riemann surface. To this end we use the celebrated Fay identity establishing the existence of trisecant points in the Kummer variety of the PPAV if the latter is a Jacobian variety. This implies the vanishing of a multi-dimensional function depending on a vector given in terms of the Abel map of four points. In the general case this vector is determined with a Newton iteration which can be performed efficiently since the function is locally holomorphic. The non-existence of a zero of his function would imply that the PPAV is not a Jacobian variety.

Eddy Brandon De Leon Aguilar
Institut de Mathématiques de Bourgogne
eddy-brandon_de-leon-aguilar@etu.u-bourgogne.fr

Christian Klein
Institut de Mathématiques de Bourgogne
Université de Bourgogne
christian.kleni@u-bourgogne.fr

Joerg Frauendiener
Department of Mathematics and Statistics
University of Otago
joerg.frauendiener@otago.ac.nz

MS25
Symmetries of Monopole Spectral Curves

The study of magnetic monopoles in gauge theory and the connection with algebraic geometry has been ongoing since the 1970s, and in 1983 Hitchin provided the criteria for certain algebraic curves to correspond to monopole solutions. These constraints are hard to solve, being transcendental in nature, and in the ensuing 40 years only a limited number of spectral curves have been discovered, typically requiring large symmetry groups. In this talk, I will present one approach to finding spectral curves using Nahm's equations and the standard Lax approach to integrable systems, highlighting how computer algebra software can dramatically simplify the non-linear part of the process. Finally, I will discuss how this combination of ideas has let us construct new charge-3 monopole spectral curves.

Linden Disney-Hogg, H. W. Braden
University of Edinburgh
a.l.disney-hogg@sms.ed.ac.uk, h.braden@ed.ac.uk

MS26
The Tropical Symplectic Grassmannian

Given a $2n$-dimensional vector space V with a symplectic form w, its linear subspace L is called isotropic if all vectors in L are pairwise orthogonal with respect to the form w. The symplectic Grassmannian is the space of all isotropic linear subspaces of V of fixed dimension. We formulate tropical analogues of several equivalent characterizations of this space and show that they are not equivalent (tropically); giving all implications between them, and some counter examples. This is joint work with Jorge A. Olarte.

George Balla
RWTH Aachen
balla@art.rwth-aachen.de

Jorge Olarte
CUNEF University, Madrid
jorge.olarte@cunef.edu

MS26
Moduli Spaces of Rational Graphically Stable Curves

We use a graph to define a new stability condition for algebraic moduli spaces of rational curves. For appropriate graphs, this new stability overlaps with weighted (Hassett) stability. We characterize when the tropical compactification of the moduli space agrees with the theory of geometric tropicalization which occurs only when the graph is complete multipartite.

Andy Fry
Whitman College
frya@whitman.edu

MS26
Tropical Fans and Normal Complexes

Associated to any divisor in the Chow ring of a simplicial tropical fan, we discuss the construction a family of polytopal complexes, called normal complexes, which we propose as an analogue of the well-studied notion of normal polytopes from the setting of complete fans. The talk will describe certain closed convex polyhedral cones of divisors for which the volume of each divisor in the conethat is, the degree of its top poweris equal to the volume of the associated normal complexes. We will discuss the theory of normal complexes developed in talk as a polytopal model underlying the combinatorial Hodge theory pioneered by Adiprasito, Huh, and Katz.

Anastasia Nathanson
University of Minnesota Twin Cities
natha129@umn.edu

Dustin Ross
San Francisco State University
rossd@sfsu.edu

MS26

Homology Represenations of Tropical Moduli Spaces

We construct, for all $g \geq 2$ and $n \geq 0$, a spectral sequence of rational S_n-representations which computes the S_n-equivariant reduced rational cohomology of the tropical moduli spaces of curves $\Delta_{g,n}$ in terms of compactly supported cohomology groups of configuration spaces of n points on graphs of genus g.

Christin Bibby
Louisiana State University
bibby@math.lsu.edu

Melody Chan
Brown University
melody_chan@brown.edu

Nir Gadish
University of Michigan
gadish@umich.edu

He Yun
MPI MiS
clyun@mis.mpg.de

MS27

Geometric Constructions From Abstract Wall-crossing

Theory of Newton-Okounkov bodies has led to the extension of the geometry-combinatorics dictionary from toric varieties to certain varieties which admit a toric degeneration. In a recent paper with Megumi Harada, we gave a wall-crossing formula for the Newton-Okounkov bodies of a single variety. Our wall-crossing involves a collection of lattices $\{M_i\}_{i\in I}$ connected by piecewise-linear bijections $\{\mu_{ij}\}_{i,j\in I}$. In addition, Kiumars Kaveh and Christopher Manon analyzed valuations into semifields of piecewise linear functions and explored their connections to families of toric degenerations. Inspired by these ideas in joint work in progress with Megumi Harada and Christopher Manon we propose a generalized notion of polytopes in $\Lambda = (\{M_i\}_{i\in I}, \{\mu_{ij}\}_{i,j\in I})$, where the M_i are lattices and the $\mu_{ij} : M_i \to M_j$ are piecewise linear bijections. Roughly, these are $\{P_i \mid P_i \subseteq M_i \otimes \mathbb{R}\}_{I\in I}$ such that $\mu_{ij}(P_i) = P_j$ for all i, j. In analogy with toric varieties these generalized polytopes can encode compactifications of affine varieties as well as some of their geometric properties. In this talk, we illustrate these ideas.

Laura Escobar
Washington University in St. Louis
laurae@wustl.edu

MS27

Khovanskii-finite Rational Curves of Arithmetic Genus Two

A common technique for studying a projective variety relies on finding a flat degeneration to a toric variety. Toric degenerations appear in a wide range of contexts, from mirror symmetry to numerical algebraic geometry. An approach to constructing such a degeneration is due to Anderson via finding a Khovanskii-finite valuation on the homogeneous coordinate ring of the variety. In this joint work with Nathan Ilten, I will talk about an algorithmic approach to deciding the existence of Khovanskii-finite valuations on rational curves of arithmetic genus two defined over a number field. We show that for this family of curves, the problem of having a toric degeneration is decidable.

Ahmad Mokhtar, Nathan Ilten
Simon Fraser University
ahmad_mokhtar@sfu.ca, nilten@sfu.ca

MS27

Newton-Okounkov Bodies of Chemical Reaction Networks

This talk introduces a new application of Newton-Okounkov body theory to the study of chemical reaction networks. An important invari- ant of a chemical reaction network is its maximum number of positive steady states, which is realized as the maximum number of positive real roots of a parametrized polynomial system. Our new upper bound on this number is the Newton-Okounkov body bound of a chemical reaction network. Explicit ex- amples demonstrate that the Newton-Okounkov body bound of a network gives a good upper bound on its maximum number of positive steady states. This Newton-Okounkov body bound is related to another upper bound, namely the mixed volume of a chemical reaction network. The Newton-Okounkov body often achieves better bounds than the mixed volume.

Elise Walker
Sandia National Laboratory
eawalke@sandia.gov

Nida K. Obatake
Texas A&M University
nobatake@tamu.edu

MS28

Modular Curves Creeping Up in Isogeny Problems

After the spectacular attacks of this summer, the panorama of isogeny based cryptography has changed. One interesting take-away from the SIKE attacks and other recent result is that ”torsion knowledge” matters. Although mostly ignored by cryptographers, a well established way to talk about torsion knowledge is the formalism of modular curves. I will explain how modular curves creep up in isogeny-based cryptography, and what they tell us about its security.

Luca De Feo
IBM Research Europe

luca@defeo.lu

MS28

Faster Supersingularity Testing

Joint work with Gustavo Banegas (Qualcomm) and Valerie Gilchrist (ULB) Supersingular elliptic curves are ubiquitous in isogeny-based cryptography. But given some elliptic curve, how can you quickly determine whether it is supersingular or not? In this talk we will compare several approaches, and describe our implementation of a new variant of Doliskani's algorithm, with a view to fast and simple CSIDH key validation.

Valerie Gilchrist
Université Libre de Bruxelles, Belgium
valerie.gilchrist@ulb.be

Benjamin Smith
INRIA and Ecole polytechnique
smith@lix.polytechnique.fr

MS28

Computing Supersingular Endomorphism Rings Using Inseparable Endomorphisms

Computing the endomorphism ring of a supersingular elliptic curve defined over a finite field is a relevant problem to cryptography, since the security of several isogeny-based cryptosystems reduces to it. Suppose we have an algorithm which generates random endomorphisms of a supersingular elliptic curve E defined over a finite field with p^2 elements. How many calls to that algorithm do we expect to make before finding enough endomorphisms to guarantee that they generate the endomorphism ring End(E) as a Z-order? In this talk we give a new heuristic argument that, using a particular kind of inseparable endomorphisms, this expectation is bounded by a constant, independent of p or E. Moreover we present an algorithm for computing End(E) which only relies on GRH and computes End(E) in expected $O(p^{(1/2+e)})$ time, for every $e > 0$.

Annamaria Iezzi
Università di Napoli
annamaria.iezzi@gmail.com

MS28

Security and Efficiency of SIDH-based Signatures

The key exchange SIDH and its corresponding key encapsulation mechanism SIKE had been the flagship isogeny-based cryptosystems before the devastating attacks by Castryck, Decru, Maino, Martindale and Robert against the hard mathematical problem on which their security is based. Nevertheless, the SIDH framework can still be used to construct secure cryptosystems, as for example digital signatures. In this talk, the security and efficiency of such SIDH-based signatures will be discussed.

Federico Pintore
Universita' di Bari
federico.pintore@gmail.com

MS29

Quantum Error Correction with a Little Help of Entanglement

The fragility of quantum mechanical systems calls to use methods of error correction when storing or sending information using quantum states. In the setting of entanglement-assisted quantum error-correcting codes (EAQECCs), the sender and the receiver have access to pre-shared entanglement, which is assumed to be noiseless. As entanglement is an additional resource, the goal is to require as little as possible. We discuss various constructions from the literature for such EAQECC based on classical error-correcting codes. Using algebraic tools, we present methods that allow to vary the amount of required entanglement. Initial tables with parameters of EAQECC for qubits and qutrits are available online at http://eaqecc.codetables.de/ The talk is partially based on joint work with Fred Ezerman, Gaojun Luo, San Ling (arXiv:2207.05647).

Markus Grassl
University of Gdansk
Poland
markus.grassl@ug.edu.pl

MS29

Duality and LP Bounds for Codes with Locality

In this talk, we take a look at the duality theory of locally recoverable codes, focusing on the applications. We introduce a class of invariants that refine the classical weight distribution and show how the locality parameter can be captured with these invariants. Moreover, we establish a duality theorem analogous to a MacWilliams identity. As an application of our results, we obtain an LP bound that improves on the best available bounds in several instances. This talk is based on joint work with Alberto Ravagnani and Benjamin Jany.

Anina Gruica, Alberto Ravagnani
Eindhoven University of Technology
a.gruica@tue.nl, a.ravagnani@tue.nl

Benjamin Jany
University of Kentucky
bja246@uky.edu

MS29

Freezing the Network Code: An Interference Alignment Problem over Finite Fields

In this seminar, we introduce a formal framework to study the multiple unicast problem for a coded network in which the network code is linear and fixed. We show that the problem corresponds to an interference alignment problem over a finite field. We then establish an outer bound for the achievable rate regions in this context and provide examples of networks where the bound is sharp. We finally give evidence of the crucial role played by the field characteristic in the problem at hand. This is a joint work with Frank Kschischang, Alberto Ravagnani and Kristen Savary.

Frank Kschischang
University of Toronto
frank@ece.utoronto.ca

Felice Manganiello
Clemson University
manganm@clemson.edu

Alberto Ravagnani
Eindhoven University of Technology
a.ravagnani@tue.nl

Kristen Savary
Clemson University
ksavary@clemson.edu

MS29
Number Theoretical Perspectives on Locally Recoverable Codes

In this talk I will cover new approaches based on the theory of global fields that allow the construction of optimal locally recoverable codes with various properties, among which hierarchy and availability.

Giacomo Micheli
University of South Florida
gmicheli@usf.edu

MS30
Using Combinatorial Designs Related to Rank Metric Codes to Construct Group Testing Matrices

A group testing matrix is a binary matrix with fewer rows than columns, where rows may represent groups or pools and columns represent samples. There is a correspondence between group testing matrices and binary superimposed codes. Superimposed codes were constructed by Kautz and Singleton in 1963 from different types of discrete structures, including Steiner triple systems and q-ary error-correcting codes. In this talk we will apply similar ideas to consider the parameters of group testing matrices that result from the q-analogs of Steiner systems and subspace transversal designs. Subspace transversal designs were introduced by Etzion and Silberstein in 2013 in connection with lifted maximum rank distance codes.

Kathryn Haymaker
Villanova University, US
kathryn.haymaker@villanova.edu

MS30
Combined Constructions for Subspace Codes

Subspace codes are the q-analog of binary block codes in the Hamming metric. Here the codewords are vector spaces over a finite field. They have e.g. applications in random linear network coding, distributed storage, and cryptography. We will describe some recent constructions for subspace codes from the literature in a general framework. We analyze the conditions under which these constructions can be combined. This way improved constructions for several parameters are obtained.

Sascha Kurz
University of Bayreuth
sascha.kurz@uni-bayreuth.de

MS30
Optimal Subspace Codes in a Schubert Variety

Subspace codes have been introduced by Koetter and Kschischang in order to tackle coding problems in the area of random linear network coding. In this framework information is encoded in subspaces of a given ambient space over a finite field. A natural metric is introduced where two subspaces are 'close to each other' as soon as their dimension of intersection is large. Subspace codes are often defined as subsets of a fixed Grassmann variety. With it comes the challenge to come up with new codes with optimal or near optimal distance and to develop efficient decoding algorithms. In this work we study subspace codes whose elements are all inside a classical Schubert variety defined over some finite field. Again one has the interesting challenge to come up with codes of maximal cardinality whose distance is at least a certain value. For some parameters we can provide subspace codes of optimal cardinality.

Gianira Alfarano
Eindhoven University of Technology
g.n.alfarano@tue.nl

Joachim Rosenthal
Institut für Mathematik
Universität Zürich
rosenthal@math.uzh.ch

Beatrice Toesca
University of Torino
beatrice.toescadicastellazzo@uzh.ch

MS30
Divisible Codes in the Rank Metric

Divisible codes in the Hamming metric have been deeply studied and attracted a lot of attention due to their connections with algebraic and geometric objects. In this talk, we will present some characterization results and constructions of divisible codes in the rank metric. We will also describe the algebraic and geometric techniques used for these results. This is a joint work with Olga Polverino, Paolo Santonastaso and John Sheekey.

Olga Polverino
University of Campania
olga.polverino@unicampania.it

Paolo Santonastaso
University of Caserta
paolo.santonastaso@unicampania.it

John Sheekey
UC Dublin
john.sheekey@ucd.ie

Ferdinando Zullo
Università degli Studi della Campania
ferdinando.zullo@unicampania.it

MS31
Determinantal Representations and the Image of the Principal Minor Map

The principal minor map takes an n by n square matrix to the length 2^n-vector of its principal minors. A basic question is to give necessary and sufficient conditions that characterize the image of various spaces of matrices under this map. In this talk I will describe the image of the space of complex matrices using a characterization of determinantal representations of multiaffine polynomials, based on the factorization of their Rayleigh differences. Using these techniques I will give equations and inequalities characterizing the images of the spaces of real and complex symmetric and Hermitian matrices. For complex symmetric matrices this recovers a result of Oeding from 2011. I will also give examples to prove that for general matrices no such finite characterization is possible. This is based on a joint work with Cynthia Vinzant.

Abeer K. Al Ahmadieh
Georgia Institute of Technology
aahmadieh@gatech.edu

Cynthia Vinzant
North Carolina State University
U.S.
vinzant@uw.edu

MS31

Alternating Minimization for Regression with Tropical Rational Functions

We propose an alternating minimization algorithm for regression over the space of tropical rational functions. The method alternates between fitting the numerator and denominator terms via tropical polynomial regression, which is known to admit a closed form solution. We demonstrate the behavior of the alternating minimization method experimentally. Our work is motivated by applications to ReLU neural networks, a popular class of network architectures in the machine learning community which are closely related to tropical rational functions. Joint work with Lars Ruthotto.

Dunbar Alex
Emory University
alex.dunbar@emory.edu

MS31

Hidden Hyperplane Convexity and Aggregations of Quadratic Inequalities

We study properties of the convex hull of a set S described by quadratic inequalities. A simple way of generating inequalities valid on S is to take nonnegative linear combinations of the defining inequalities of S. We call such inequalities *aggregations*. Special aggregations naturally contain the convex hull of S, and we give sufficient conditions for intersection of such aggregations to define the convex hull. We introduce the notion of hidden hyperplane convexity (HHC), which is related to the classical notion of hidden convexity of quadratic maps. We show that if the quadratic map associated with S satisfies HHC, then the convex hull of S is defined by special aggregations. To the best of our knowledge, this result generalizes all known results regarding aggregations defining convex hulls. Using this sufficient condition, we are able to recognize previously unknown classes of sets where aggregations lead to convex hull. We show that under a stronger assumption, finitely many aggregations always suffice to define the convex hull, answering a question raised in [Dey, Munoz, Serrano 2021]. All the above results are for sets defined using open quadratic inequalities. For closed quadratic inequalities, we prove a new result regarding aggregations giving the convex hull, without topological assumptions on S, which were needed in previous works.

Shengding Sun
Georgia Institute of Technology
Georgia Institute of Technology
ssun313@gatech.edu

Greg Blekherman, Santanu Dey
Georgia Institute of Technology
gblekherman3@gatech.edu, santanu.dey@isye.gatech.edu

MS32

On Taylor Polynomials of Rational Functions

The topic of the talk evolves around the following question: which polynomials of degree m in n variables are the Taylor polynomials of a rational function of degree (d, e)? In other words, what conditions must satisfy the coefficients of a polynomial to let it be the Taylor expansion of a rational function? For every choice of the parameters (n, d, e, m) this defines a projective variety in the set of degree m polynomials, that we call the Taylor variety. In the talk I will present some results concerning the dimension theory and remarkable properties of Taylor varieties. The main motivation comes from numerical analysis, precisely, from the so-called Pad approximation problem, where the polynomial is the Taylor polynomial of a regular function around the origin, and one looks for a rational function of low degree that has the same Taylor polynomial. Joint work with A. Conca, G. Ottaviani and B. Sturmfels.

Simone Naldi
Université de Limoges
simone.naldi@unilim.fr

Aldo Conca
Department of Mathematics
University of Genova
conca@dima.unige.it

Giorgio Ottaviani
University of Firenze
giorgio.ottaviani@unifi.it

Bernd Sturmfels
MPI Leipzig and UC Berkeley
bernd@mis.mpg.de

MS32

The Christoffel-Darboux Kernel for Topological Data Analysis

In topological data analysis, persistent homology has been widely used to study the topology of point clouds in R^n. Unfortunately, standard methods are very sensitive to outliers, and their computational complexity depends badly on the number of data points. In this talk we will present a novel persistence module, based on recent applications of Christoffel-Darboux kernels in the context of statistical data analysis and geometric inference. Our approach is robust to outliers and can be computed in time linear in the number of data points. We illustrate the benefits and limitations of our new module with various numerical examples in R^n, $n = 1, 2, 3$.

Pepijn Roos Hoefgeest
Vrije Universiteit Amsterdam
p.e.r.rooshoefgeest@vu.nl

MS32

Computing the Conditional Expectation from Moments

We investigate the following problem: Given the moments of two random variables X and Y, can we compute the conditional expectation of X given Y? We show that this question can be answered positively if the distributions of X and Y are moment-determinate. In that case, we show that the conditional expectation of X given Y can be computed via a linear, but infinite dimensional, system of equations on the moments of X and Y. We further show that finite dimensional truncations of this system of linear equations give rise to a converging approximation of the conditional expectation.

Corbinian Schlosser
LAAS-CNRS, Toulouse
corbinian.schlosser@laas.fr

MS32

Towards Breaking the Curse of Dimension in Smooth Optimal Transport

We show how to break the curse of dimension for the estimation of optimal transport distance between two smooth distributions for the Euclidean squared distance. The approach relies on essentially one tool: represent inequality constraints in the dual formulation of OTby equality constraints with a sum of squares in reproducing kernel Hilbert space. By showing this representation is tight in the variational formulation, one can then leverage smoothness to break the curse.

François-Xavier Vialard
Univ. Gustave Eiffel
francois-xavier.vialard@univ-eiffel.fr

MS33

Inverse Problems in Persistent Homology

Persistent homology (PH) is a celebrated algorithm in topological data analysis which takes as input a topological space equipped with a real valued function and returns a barcode, a multiset of intervals in the real line. Barcodes arising from geometric data are often used for classification. It is therefore natural to ask how much information is lost by applying PH: what is the space of functions on a fixed topological space whose persistent homology is a given barcode? We discuss novel approaches recently developed to answer this question in different settings.

David Beers
University of Oxford
david.beers@maths.ox.ac.uk

MS33

Grounded Persistent Path Homology - a Stable, Topological Descriptor for Weighted Digraphs with Applications to Vascular Networks

Weighted digraphs are used to model a variety of natural systems and can exhibit interesting structure across a range of scales. In order to understand and compare these systems, we require stable, interpretable, multiscale descriptors. To this end, we propose grounded persistent path homology (GrPPH) - a new, functorial, topological descriptor that describes the structure of an edge-weighted digraph via a persistence barcode. We show there is a choice of circuit basis for the graph which yields geometrically interpretable representatives for the features in the barcode. Moreover, we show the barcode is stable, in bottleneck distance, to both numerical and structural perturbations. To conclude, we use the new descriptor to study numerical simulations of vascular flow in model tumours.

Thomas Chaplin
University of Oxford
thomas.chaplin@maths.ox.ac.uk

MS33

Topological Parameter Inference and Model Selection

One way to evaluate the quality of a mathematical model is to assess its ability to reproduce observed data. For models which produce spatial, temporal and multi-scale data, novel techniques of data analysis are needed to perform this comparison. We combine topological data analysis with Bayesian statistics to study the problems of parameter inference and model selection. We study angiogenesis - the process by which new blood vessels form from an existing network - and compare the spatial properties of different models. Our work provides a general framework for analysing spatial models, which may be applied in other scenarios by choosing from a variety of filtrations, vectorisations and summary statistics.

Robert McDonald
University of Oxford
robert.mcdonald@maths.ox.ac.uk

MS33

Reverse Engineering Discrete Time Continuous Space Biological Dynamical Systems

We describe a technique for finding wiring diagrams from data for discrete time, continuous space dynamical systems, where the functions are monotone increasing or decreasing in each variable (which most functions coming from biology seem to satisfy). The methods use computational and commutative algebra. We also investigate the situation of random uniform small error in measurements, and show that for enough data, for small enough error, the correct wiring diagram will be found. This represents joint work with Heather Harrington and Alan Veliz-Cuba (arXiv:2212.02601).

Heather Harrington
Mathematical Institute
University of Oxford
harrington@maths.ox.ac.uk

Michael Stillman
Cornell University
mike@math.cornell.edu

Alan Veliz-Cuba
Department of Mathematics
University of Dayton
avelizcuba1@udayton.edu

MS34

Bayesian Integrals on Toric Varieties

Some statistical models are naturally parameterized by the positive part of a toric variety, which I demonstrate with the example of a gambler. In order to be able to compute Bayesian integrals for such models, we endow toric varieties with probability measures. The latter are motivated from positive geometries in high energy physics. This talk is based on joint work with M. Borinsky, B. Sturmfels, and

S. Telen. Exploiting the combinatorial nature of toric varieties, we provide algorithms to sample from densities on toric varieties.

Michael Borinsky
ETH-ITS
michael.borinsky@eth-its.ethz.ch

Anna-Laura Sattelberger
KTH Royal Institute of Technology
alsat@kth.se

Bernd Sturmfels
MPI Leipzig and UC Berkeley
bernd@mis.mpg.de

Simon Telen
MPI MiS Leipzig
simon.telen@mis.mpg.de;

MS34

Connectivity of the Parameter Region of Multistationarity in Reaction Networks, and Beyond

Despite recent developments, describing the set of parameters that enable multistationarity in a chemical reaction network is a challenging problem. Under certain assumptions on the network, one can associate a critical polynomial to the network that gives information about multistationarity. Especially, one can use the critical polynomial to study the shape of the parameter region of multistationarity, in particular, its connectivity. Motivated by this setting, we give conditions based on the geometrical configuration of the exponents and the sign of the coefficients of a polynomial that guarantee that the number of connected components of the complement of the hypersurface where the defining polynomial attains a negative value is at most one or two.

Máté L. Telek, Elisenda Feliu
University of Copenhagen
mlt@math.ku.dk, efeliu@math.ku.dk

MS34

The Anchored Line Multiview Variety and Line Segment Reconstruction

The 3D image reconstruction problem aims to create a tridimensional model of a scene from 2D images. In order to do so, point and line features are identified and matched in the images, creating correspondences that are used to triangulate each feature in space, and recreate the scene. In this talk we will focus on the triangulation of incident points and lines. We define the *Anchored Multiview varieties* as restrictions of the well known point and line multiview varities, with the goal of modelling the presence of point and line incidences. We will present the basic properties of these varieties and give formulas for their Euclidean Distance Degrees. We also present numerical experiments comparing the triangulation of points incident to a line, using different methods involving anchored multiview varieties.

Angelica Torres
Centre de Recerca Matemàtica
atorres@crm.cat

Felix Rydell
KTH
felixry@kth.se

Elima Shehu
MPI MiS Leipzig and University of Osnabrück
elima.shehu@mis.mpg.de

MS34

Invariant Polynomials in Optimization and Real Algebraic Geometry

Many important polynomial systems have additional structure, for example, generating polynomials invariant under the action of the symmetric group. In this talk we consider two problems for such systems. The first focuses on computing the critical points of a polynomial map restricted to an algebraic variety, a problem which appears in many application areas including polynomial optimization. Our second problem is to decide the emptiness of algebraic varieties over real fields, a starting point for many computations in real algebraic geometry. In both cases we provide efficient probabilistic algorithms for which take advantage of the special invariant structure.

Thi Xuan Vu
The Arctic University of Norway
thi.x.vu@uit.no

Jean-Charles Faugere
Salsa project, INRIA Paris-Rocquencourt
jean-charles.faugere@inria.fr

George Labahn
University of Waterloo
glabahn@uwaterloo.ca

Cordian Riener
UiT The Arctic University of Norway
cordian.riener@uit.no

Mohab Safey El Din
Sorbonne University, France
Mohab.Safey@lip6.fr

Eric Schost
Cheriton School of Computer Science
University of Waterloo
eschost@uwaterloo.ca

MS35

Eigenvectors of Tensors: Recent Developments

Eigenvectors of tensors, extensions of eigenvectors of matrices, were introduced by H. Lim and L. Qi independently in 2005 and have been studied in numerical multilinear algebra. Recently, the concept of tensor eigenvectors drew attention from the algebraic geometry community because algebraic geometry has proven to provide useful techniques for the tensor eigenproblem. The purpose of this talk is to discuss recent developments in spectral theory of tensor eigenvectors.

Hirotachi Abo
University of Idaho

abo@uidaho.edu

MS35

Maximal Border Subrank Tensors

Subrank and border subrank were introduced by Strassen. The rank and border rank of a generic tensor are the same and equal to the maximal border rank. However, we know less about the behavior of the subrank and border subrank. In this talk, we will introduce subrank and border subrank. Then we will give a lower bound of the dimension of the set of maximal border subrank tensors.

Chia-Yu Chang
Texas A&M University
chiayu@tamu.edu

MS35

Restrictions of Tensors over Finite Fields

Restriction is a natural quasi-order on d-way tensors. We establish a remarkable aspect of this quasi-order in the case of tensors over a fixed finite fieldnamely, that it is a well-quasi-order: it admits no infinite antichains and no infinite strictly decreasing sequences. This result, has consequences for an arbitrary restriction-closed tensor property X, including tensor rank (analytic rank, asymptotic rank,...) smaller or equal than a given number. For instance, X admits a characterisation by finitely many forbidden restrictions and can be tested by looking at subtensors of a fixed size. We proved that a generalisation of the tensor restriction theorem to other such representations (e.g. homogeneous polynomials of a fixed degree) is also true. The talk is based on a joint work with Andreas Blatter and Jan Draisma.

Filip Rupniewski
Bern University
filip.rupniewski@unibe.ch

MS35

Signature Tensors of Paths and Their Representation Theory

In stochastic analysis, a standard method to study a path X is to work with its signature, which is a sequence of tensors that encode in a compact form the information carried by X. The set of tensors that arise as the signatures of paths can be given the structure of an algebraic variety, called universal variety. This allows us to use powerful geometric techniques to study paths. After a suitable change of coordinates, the universal variety is a weighted analogue of the Veronese variety. Viewing this change of coordinates from the point of view of representation theory naturally leads us to some deep problems in algebraic combinatorics. In my talk I will report on a work in progress, joint with Carlos Amndola, Francesco Galuppi, Angel Rios and Pierpaola Santarsiero, where we explore these interactions between algebraic geometry, representation theory, algebraic combinatorics, and signature tensors.

Carlos E. Amendola Ceron
Technical University Munich
amendola@math.tu-berlin.de

Francesco Galuppi
Polish Academy of Sciences
fgaluppi@impan.pl

Angel Rios Ortiz
Max Planck Institute for Mathematics in the Sciences
angel.rios@mis.mpg.de

Pierpaola Santarsiero
University of Trento
pierpaola.santarsiero@mis.mpg.de

Tim Seynnaeve
KU Leuven
tim.seynnaeve@kuleuven.be

MS36

Efficient Computation of Macaulay Matrix Nullspaces Through Exploiting Shift-Invariant Structures

In this talk, we discuss the problem of efficiently computing the right-nullspace of the Macaulay matrix, which is a crucial step in many polynomial systems root-solving algorithms. For an overdetermined bivariate polynomial system Σ with $S \geq 2$ equations of degree d_Σ, the complexity of computing a nullspace containing all system roots is $O(d_\Sigma^6)$ using standard algorithms (e.g., SVD, rank-revealing QR). We however show that it is possible to reduce the complexity to $O(d_\Sigma^5)$ if one is willing to exploit the shift-invariant structures in the Macaulay matrix. By converting the Macaulay matrix into a Cauchy-like matrix using Fourier transforms, we devise an algorithm that efficiently determines the nullspace from a rank-revealing LU factorization using the celebrated Schur algorithm. Since the algorithm relies on Gaussian elimination to compute the nullspace, interesting parallels to Grbner basis computations can be drawn. Details of the proposed method, including stability considerations, are covered in the talk. Also discussed are generalizations of the fast algorithm to polynomial systems expressed in the Chebyshev basis and the difficulties involved with extending the fast algorithm to general n-variable systems.

Nithin Govindarajan
KU Leuven
nithin.govindarajan@kuleuven.be

MS36

Galois/M onodromy Groups for Decomposing Minimal Problems in 3D Reconstruction

Many problems in computer vision are represented using a parameterized polynomial system, where the solution set is critical for 3D reconstruction. Minimal problems can be of special interest as these polynomial systems are well-constrained and generically have finitely many solutions. Computing the Galois/monodromy group of the associated branch cover can yield information and understanding about the underlying structure of the minimal problem. One potential outcome of this computation is identifying possible decompositions or symmetries that enable more efficient solution solving. These Galois/monodromy groups can be computed using numerical homotopy continuation via a multitude of softwares. Examples such as the classical homography estimation and five-point relative pose problems will be provided to show these computations and the structure they can help identify. This is joint work with Timothy Duff, Viktor Korotynskiy, and Tomas Pajdla.

Margaret H. Regan
Duke University
Durham, NC USA

mregan@math.duke.edu

MS36

Condition-Based Probabilistic Complexity of Symbolic Algorithms: Descartes' Solver and Beyond!

Condition-based complexity is a fundamental complexity paradigm in numerical computation, where the complexity of algorithms is doomed to depend not only on the input-size but also on the conditioning of the inputi.e., how sensitive the problem is with respect to variations of the given input. In contrast, in symbolic computation, the usual complexity paradigm is the so-called worst-case complexity where the complexity of an algorithm is bounded exclusively in terms of the input-size alone. A great advantage of condition-based complexity analysis is that they lead easily to probabilistic complexity analyses. These analyses allow us to understand the statistics of the practical behavior of the algorithm. In this talk, we explore how to use condition-based complexity analyses in the symbolic world as we do in the numerical world. In other words, we will show how to use condition numbers to understand the probabilistic run-time of symbolic algorithms, and so the statistics of their behavior in practice.

Josué Tonelli-Cueto
The University of Texas at San Antonio
josue.tonelli.cueto@gmail.com

Elias Tsigaridas
Inria Paris
elias.tsigaridas@inria.fr

Alperen Ergur
University of Texas, San Antonio
alperen.ergur@utsa.edu

MS36

Computations With and About the Resultant System

The resultant is one of the most fundamental objects in computational algebraic geometry. There are plenty of definitions for different cases and even more construction methods. In ”Modern Algebra”, given a system of polynomials S (without very restrictive conditions on the number of variables or equations) van der Waerden constructs a system of polynomials R with the property that R is feasible if and only if S is feasible. Since this mimics the most intuitive definition of resultant, van der Waerden calls this system ”the resultant system”. Following the standard construction where the resultant system is the set of coefficients of $Res\left(\sum_{i=1}^{m} u_i f_i, \sum_{i=1}^{m} v_i f_i\right)$ when viewed as a polynomial in the u_i and v_i variables, the number of elements in the resultant system is enormous. Nevertheless, we observe that there is a large number of repetitions due to symmetry. Moreover, some of the coefficients are combinations of others and thus not needed in the resultant system. After an analysis of such redundancies, we argue that the resultant system is a useful tool in real algebraic geometry, both in theory and in practice. We provide combinatorial computations for the number of elements in the resultant system for some polynomial systems of low degree. In computing elimination ideals, we show that for some cases computing the resultant system first improves the performance.

Zafeirakis Zafeirakopoulos
Section de mathématiques - Université de Genève
zafeirakis.zafeirakopoulos@unige.ch

MS37

Adaptive Mapper

Mapper is a popular topological data visualization tool that takes as input a set of point cloud data and produces as output a one-dimensional graph reflecting the structure of the underlying data. To use Mapper, the user must specify many parameters to get the output graph. This includes choosing a lens function from a point cloud X to a lower-dimensional space Y, an open cover of the target space Y, and a clustering algorithm. Optimizing these parameters is an essential part of obtaining a nice Mapper graph but are often challenging to find. We focus on parameter selection, especially tuning an open cover which is often a collection of overlapping intervals or hypercubes. We propose a new algorithm for learning an open cover that is based on clustering algorithms, statistical tests, and an iterative splitting procedure. Additionally, we provide an algorithm for learning an open cover on a modification of Mapper called Ball Mapper. We compare our algorithms to state-of-the-art techniques and present some stability results.

Robin Belton
Smith College, U.S.
rbelton@smith.edu

Sarah Percival
Michigan State University
perciva9@msu.edu

Enrique Alvarado
University of California Davis
ealvarado@math.ucdavis.edu

Sourabh Palande, Sarah Tymochko
Michigan State University
palandes@msu.edu, tymochko@math.ucla.edu

Emilie Purvine
Pacific Northwest National Laboratory
emilie.purvine@pnnl.gov

Kang-Ju Lee
Seoul National University
leekj0706@snu.ac.kr

Emily Fischer
Umpqua Bank
fischer_emily@wheatoncollege.edu

MS37

A Condition for the Uniqueness of Frchet Means of Persistence Diagrams

The Frchet mean is an important statistical summary which has been defined and studied for sets of persistence diagrams. It has been established that the Frchet mean for sets of persistence diagrams is non-unique due to the non-negative curvature of persistence diagram space. There is currently no criterion to determine when, if ever, the Frchet mean of a set of persistence diagrams is unique. We propose a condition of flatness on groupings of persistence diagrams and prove that this condition yields a unique Frchet mean for a set of persistence diagrams. Furthermore, for discrete probability measures supported on flat groupings of persistence diagrams, we prove that the empirical Frchet mean converges to the population Frchet mean at a rate of $O(n^{-\frac{1}{2}})$, where n is the number of samples.

Yueqi Cao, Anthea Monod
Imperial College London
y.cao21@imperial.ac.uk, a.monod@imperial.ac.uk

MS37

Tda for Spatial Systems Biology

Biological processes are multi-scale. Spatial structures and patterns vary across levels of organisation, from molecular to multi-cellular to multi-organism. With more sophisticated mechanistic models and data available, quantitative tools are needed to study their evolution in space and time. Topological data analysis (TDA) provides a multiscale summary of data. Here we present extensions to the persistent homology pipeline and highlight its utility with concrete case studies arising in biological systems.

Heather Harrington
Mathematical Institute
University of Oxford
harrington@maths.ox.ac.uk

MS37

Noise Robustness of Persistent Homology in Practice

Topological data analysis is a recent and fast growing field that approaches the analysis of data sets using techniques from (algebraic) topology. Its main tool, persistent homology (PH), has seen a notable increase in applications in the last decade. Often cited as the main reason behind the recent popularity of PH in data analysis is its proven stability, which is described as a theoretical guarantee of noise robustness, and of crucial importance due to the unavoidable presence of noise or measurement error in real data. However, little attention has been paid to what these stability theorems mean in practice. To gain some insight into this question, we evaluate the noise robustness of PH on the MNIST dataset of greyscale images. More precisely, we investigate to what extent PH changes under typical forms of image noise, and quantify the loss of performance in classifying the MNIST handwritten digits when noise is added to the data. The results show that the sensitivity to noise of PH is influenced by the choice of filtrations and persistence signatures (respectively the input and output of PH), and in particular, that PH features are often not robust to noise in a classification task.

Renata Turkes
University of Antwerp
renata.turkes@hotmail.com

Jannes Nys
École polytechnique fédérale de Lausanne
jannes.nys@epfl.ch

Tim Verdonck, Steven Latré
University of Antwerp
tim.verdonck@uantwerpen.be, steven.latre@uantwerpen.be

MS38

From Translation Surfaces to Algebraic Curves

We study constructing an algebraic curve from a Riemann surface given via a translation surface, which is a collection of finitely many polygons in the plane with sides identified by translation. We use the theory of discrete Riemann surfaces to give an algorithm for approximating the Jacobian variety of a translation surface whose polygon can be decomposed into squares. We first implement the algorithm in the case of L shaped polygons where the algebraic curve is already known. The algorithm is then implemented for a family of translation surfaces called Jenkins–Strebel representatives that, until now, lived squarely on the analytic side of the transcendental divide between Riemann surfaces and algebraic curves. Using Riemann theta functions, we give numerical experiments and resulting conjectures up to genus 5.

Samantha Fairchild
MPI MiS Leipzig
skayf92@gmail.com

Yelena Mandelshtam
UC Berkeley
yelenam@berkeley.edu

Türkü zlüm elik
Simon Fraser University
turkuozlum@gmail.com

MS38

From Schottky Groups to Algebraic Curves

Schottky groups uniformize algebraic curves, and their moduli space sits as an intermediate between the moduli space of curves (algebraic) and the Teichmuller space (analytic). I will present joint work with Samantha Fairchild and Alex Elzenaar where we compute (an approximation of) the canonical ideal of an algebraic curve given in terms of Schottky data.

Angel Rios Ortiz
Max Planck Institute for Mathematics in the Sciences
angel.rios@mis.mpg.de

MS38

Reconstructing Curves from Their Period Matrices

An algebraic curve over a number field equipped with a basis of differentials gives rise to a ”big” period matrix, which can be normalized further by forgetting the specific basis of differentials, leading to a ”small” period matrix. We discuss how the algebraic curve can be reconstructed from both kinds of period matrix, in the latter case over CC and in the former case over the original number field. The algorithms use results by Gurdia, Balakrishnan–Ionica–Lauter–Vincent, and Lercier–Ritzenthaler.

Jeroen Sijsling
University of Ulm
jeroen.sijsling@uni-ulm.de

MS38

Reconstruction of Curves From Their Theta Hy-

perplanes in Genera 6, 7

We derive a closed formula for the ideal of enveloping quadrics of a generic canonical curve C of genus 6 or 7 in terms of the theta hyperplanes of C. This data suffices to reconstruct the curve. Hence, we get a generic inverse to the Torelli map, as well as a complete description of the Schottky locus in these genera. The computational part of the proof is a certified numerical argument. Joint w/ T. . elik

Türkü zlüm elik
Simon Fraser University
turkuozlum@gmail.com

David Lehavi
Resonai
dlehavi@gmail.com

MS39

Counting Tropical Curves in $\mathbb{P}^1 \times \mathbb{P}^1$: Computation & Polynomiality Properties

By the celebrated correspondence theorem of Mikhalkin, counting curves in $\mathbb{P}^2$ with prescribed numerical restrictions can be achieved by counting tropical curves with similar numerical restrictions, and in turn, by counting lattice paths in a triangle with a suitable multiplicity function. This correspondence readily generalizes to any smooth toric surface. We implement Mikhalkin's lattice path algorithm for an arbitrary lattice polygon and with arbitrary boundary conditions in Polymake, and use this to determine new polynomial structures on counts of rational curves in $\mathbb{P}^1 \times \mathbb{P}^1$ with fixed contact orders to the 0 and infinity sections, and variable contact orders to the 0 and infinity fibers. This is based on joint work with Hannah Markwig and Dhruv Ranganathan.

Daniel J. Corey
Technische Universität Berlin
dcorey2814@gmail.com

Hannah Markwig
Universität Tübingen
hannah.markwig@uni-tuebingen.de

Dhruv Ranganathan
University of Cambridge
dr508@cam.ac.uk

MS39

Finding Generic Root Counts of Polynomial Systems Using Tropical Geometry

A famous result by Bernstein says that the number of solutions to a square system of polynomial equations with generic monomial supports is given by a combinatorial invariant known as the mixed volume. In this talk, I will discuss how we can use tropical intersection theory to go beyond this theorem and tackle a wide variety of new systems, including those coming from applications such as chemical reaction networks. In this case, the generic root count is given by the matroidal degree of a binomial variety, which in many cases is highly computable. The idea is to study the variation of tropical structures in algebraic families. We show that if a family is suitably well behaved (tropically flat), then the behavior of a single tropicalization spreads to an open dense subset, thus giving generic behavior. This in particular gives a concrete combinatorial criterion to check if the generic root count of a system is a tropical intersection number. I will show that we can apply this to a wide variety of systems, including the steady-state equations of chemical reaction networks and the polynomial systems studied by Kaveh and Khovanskii. This in particular gives a tropical formula for the volumes of Newton-Okounkov bodies. This is joint work with Yue Ren. For applications in chemical reaction network theory, I am working together with Yue Ren, Elisenda Feliu, Benjamin Schrter, Oskar Henriksson and Mt Telek.

Paul Helminck
Durham University
paul.a.helminck@durham.ac.uk

MS39

Tropical Methods in $\mathbb{A}^1$-Enumerative Geometry

In enumerative geometry one counts geometric objects, for example points, lines, curves etc., satisfying certain algebraic conditions. This is classically done over the complex or the real numbers. Methods from $\mathbb{A}^1$-homotopy theory allow to get a meaningful answer to these questions over an arbitrary base field and the resulting area is called $\mathbb{A}^1$-enumerative geometry. In my talk I will explain how to use tropical geometry to attack questions in $\mathbb{A}^1$-enumerative geometry.

Andrés Jaramillo Puentes
University of Duisburg-Essen, Germany
andres.jaramillo-puentes@uni-due.de

Sabrina Pauli
Universitaet Duisburg-Essen
sabrina.pauli@uni-due.de

MS39

Computing the Dimension of the Semirings of Polynomials and Convergent Power Series

In this talk I will define the Krull dimension of a (topological) semiring as the number of strict inclusions in a chain of prime congruences. I will compute the dimensions of the polynomial semirings with coefficients in the tropical numbers or in any of its sub-semifields. I will also give bounds for the dimension of the semiring of convergent power series with coefficients in the tropical numbers or any of its sub-semifields. These computations are very explicit and involve looking at the ranks of certain matrices. I will explain how these computations align with our geometric intuition (from tropical geometry).

Kalina Mincheva, Netanel Friedenberg
Tulane University
kmincheva@tulane.edu, nfriedenberg@tulane.edu

MS40

Applications of Grassmannians and Flag Manifolds

I will briefly introduce flag manifolds (including the special case of Grassmannians), and survey some applications, from signal processing to polymer modeling to data science.

Clayton Shonkwiler
Department of Mathematics
Colorado State University

clayton.shonkwiler@colostate.edu

MS41

Breaking the Supersingular Isogeny Diffie-Hellman Protocol

Finding an explicit isogeny between two given isogenous elliptic curves over a finite field is considered a hard problem, even for quantum computers. In 2011 this led Jao and De Feo to propose a key exchange protocol that became known as SIDH, short for Supersingular Isogeny Diffie-Hellman. The security of SIDH does not rely on a pure isogeny problem, due to certain ”auxiliary” elliptic curve points that are exchanged during the protocol (for constructive reasons). In 2017 SIDH was submitted to the NIST standardization effort for post-quantum cryptography, and since then it has attracted a lot of attention. Early July, it advanced to the fourth round. In this talk I will discuss a break of SIDH that was discovered in collaboration with Thomas Decru about three weeks later. The attack uses isogenies between abelian surfaces and exploits the aforementioned auxiliary points, so it does not break the pure isogeny problem. It allows for a full key recovery at the highest security level in a few hours. As time permits, I will also discuss some more recent improvements and follow-up work due to Maino et al. and Robert.

Wouter Castryck
KU Leuven
Ghent University
wouter.castryck@gmail.com

MS41

The Fall of SIKE: One Year Later

Almost exactly one year ago, Wouter Castryck and I broke Microsofts $IKEp217 challenge by using isogenies between abelian surfaces based on a reducibility criterion by Kani. Even though this lead to the ultimate demise of SIKE as one of NISTs post-quantum standardization candidates, it also opened up a new and exciting direction in which isogeny-based cryptography could steer. In this talk we will give an overview of the impact of Kanis theorem from the past year, and discuss possible future challenges and opportunities.

Thomas Decru
KU Leuven
thomas.decru@kuleuven.be

MS41

At the Evening of SIDH Attacks

In summer 2022, SIKE, SIDH and derived schemes were broken in polynomial time by a series of papers (Wouter Castryck and Thomas Decru, Luciano Maino and Chloe Martindale, and Damien Robert). In this talk, we discuss the countermeasure ideas that have appeared till date, and have a brief overview of their security.

Tako Boris Fouotsa
EPFL
tako.fouotsa@epfl.ch

MS42

The Diagonals of Ferrers Diagrams

In 1986, Garsia and Remmel defined the q-rook polynomials for Ferrers diagrams. They showed that they share many properties with the rook numbers introduced by Riordan and Kaplansky. In 1998, Haglund enstablished connections between q-rook polynomials and matrices over finite fields. In this talk, we reconstruct the theory of q-rook polynomials for Ferrers diagrams by focusing on the properties of their diagonals. We show that the diagonals define an equivalent relation on the set of Ferrers diagrams and we establish connections with the problem of counting matrices of given rank supported on a Ferrers diagram.

Giuseppe Cotardo
Virginia Tech
gcotardo@vt.edu

Anina Gruica, Alberto Ravagnani
Eindhoven University of Technology
a.gruica@tue.nl, alberto.rvgn@gmail.com

MS42

Codes From Grassmann and Schubert Varieties

The codes from Schubert varieties, a natural generalization of the codes from Grassmann varieties, have drawn the attention of several mathematicians in the recent past. In this talk, we will review the known results regarding some known parameters of these codes (such as dimensions and minimum distance) and present recent developments on a conjecture related to the characterization of minimum distance codewords of these codes by Ghorpade and Singh. We will also present recent results on the generalized Hamming weights of the codes from Schubert varieties. This is a joint work with Sudhir Ghorpade and Avijit Panja.

Mrinmoy Datta
Indian Institute of Technology Hyderabad
mrinmoy.datta@math.iith.ac.in

MS42

On the Algebraic Structure of Quasi-cyclic Codes and Galois Invariance

Quasi-cyclic codes over finite fields constitute an important family of linear block codes. Some quasi-cyclic codes with additional properties are being used in practical applications like 5G or to propose post-quantum cryptographic algorithms. Due to this, the algebraic structure of quasi-cyclic codes have been investigated amply. In particular, it is known that every quasi-cyclic code has a reduced Grbner basis. In this work, we use this unique basis to introduce the notion of zeros of quasi-cyclic codes. By means of these, we provide an algebraic construction of a generator and a parity check matrix for a quasi-cyclic code over an extension field. We show that this new quasi-cyclic code has the same parameters as the original one and that it is Galois invariant. The trace of the Galois invariant code coincides with its subfield subcode and either allows to recover the quasi-cyclic code over the base field.

Julia Lieb
University of Zurich
julia.lieb@math.uzh.ch

Henry Chimal-Dzul
University of Notre Dame
hchimald@nd.edu

Joachim Rosenthal
Institut für Mathematik

Universität Zürich
rosenthal@math.uzh.ch

MS42

A Computational Single-server Private Information Retrieval Scheme From Codes Over Rings

A Private Information Retrieval (PIR) scheme allows users to retrieve data from a database without disclosing to the server information about the identity of the data retrieved. A single-server PIR protocol requires computational difficulty. That is, if data is stored in a single database, one can only guarantee information-theoretic privacy by downloading the full database, which has a high communication cost. The first computational PIR scheme based on linear codes was introduced in [2020 IEEE International Symposium on Information Theory (ISIT), pp. 10651070 (2020] by Holzbaur, Hollanti and Wachter-Zeh. However, Bordage and Lavauzelle presented an attack in [Cryptogr. Commun. 13, 519526 (2020)]. In this work, we present a modified version of the previous scheme, that uses codes over rings, which is resistant to the attack in [Cryptogr. Commun. 13, 519526 (2020)].

Seyma Bodur
IMUVA-Mathematics Research Institute University of Vallado
seyma.bodur@uva.es

Edgar Martinez-Moro
Institute of Mathematics
University of Valladolid
edgar.martinez@uva.es

Diego Ruano
IMUVA-Mathematics Research Institute
University of Valladolid, Spain
diego.ruano@uva.es

MS43

On the List Decodability of Derivative Codes

The famous Guruswami-Sudan list decoding algorithm of Reed-Solomon reaches the Johnson radius. Efforts have later been produced to improve this radius and reach the capacity of list decoding. This was achieved by Guruswami using Folded Reed-Solomon codes with multivariate high degree interpolation, later simplified with a linear-algebraic list decoding algorithm. It is striking that, while the standard Guruswami-Sudan list decoding algorithm is field agnostic and does not rely on any hypothesis on the underlying field, the high degree interpolation based and the linear-algebraic list decoding algorithms both need the finiteness of the underlying field to obtain a bound on the size of list. In this talk, we show a few cases of regimes of the auxiliary m and s parameters where the list size can be established with no hypothesis of finiteness of the underlying field. Joint work with Alain Couvreur, Emmanuel Hallouin, Thierry Henocq, Marc Perret

Daniel Augot
INRIA
daniel.augot@inria.fr

Alain Couvreur
INRIA Saclay
alain.couvreur@inria.fr

Emmanuel Hallouin, Thierry Henocq, Marc Perret
Institut de Mathématiques de Toulouse
hallouin@univ-tlse2.fr, henocq@univ-tlse2.fr, perret@univ-tlse2.fr

MS43

CSS-T Codes from Reed-Muller Codes for Quantum Fault-Tolerance

Fault-tolerant quantum computation is a critical step in the development of practical quantum computers. Unfortunately, not every quantum error-correcting code can be used for fault-tolerant computation. Rengeswamy et. al. define CSS-T codes, which are CSS codes that admit a physical transversal T-gate. In this talk we give a comprehensive study of CSS-T codes from Reed-Muller codes. These codes allow for the construction of CSS-T code families with non-vanishing asymptotic rate and possibly diverging minimum distance, desirable properties for fault-tolerant quantum computation. This work was partially supported by the National Science Foundation under grant DMS-1547399.

Jessalyn Bolkema
California State University, Dominguez Hills
jbolkema@csudh.edu

Felice Manganiello
Clemson University
manganm@clemson.edu

MS43

Homomorphic Encryption for Error Correction

Homomorphic encryption can allow verification that a vector pertains to a subspace without the need to have the full basis of that subspace. Such a variant on Diffie-Hellman, proposed by Zhao et al., provides security against Byzantine attacks, by transmission of a vector orthogonal to the subspace spanned by the message vectors. In this work, we show how to provide correction to random noise for concatenated codes where the inner codes are decoded by using guessing random additive noise decoding (GRAND) proposed by Duffy et al. Inner codes are decoded via GRAND and verified as being part of the subspace of message vectors via the orthogonal vector. Component codes that pass the homomorphic test are kept, whereas component codes that do not are further decoded by GRAND or are treated as erasures. The outer MDS code is used to recover the original messages as long as the number of inner codes that are treated as erasures is below the erasure correcting capabilities of the outer code. We show the usefulness of the scheme under burst jamming attacks.

Ken Duffy
Northeastern University
k.duffy@northeastern.edu

Muriel Medard, Peihong Yuan
Massachusetts Institute of Technology
medard@mit.edu, phyuan@mit.edu

MS43

Coded Distributed Batch Matrix Multiplication via an Additive Combinatorics Lens

Fault tolerance is a major concern in distributed computational settings. In the classic master-worker setting, a server (the master) needs to perform some heavy computation which it may distribute to n other machines (workers) in order to speed up the time complexity. In this setting, it is crucial that the computation is made robust to failed workers, in order for the master to be able to retrieve the result of the joint computation despite failures. A prime complexity measure is thus the *recovery threshold*, which is the number of workers that the master needs to wait for in order to derive the output. In this talk, I address the fundamental and well-studied task of matrix multiplication; i.e., when the master needs to multiply a batch of n pairs of matrices. Several coding techniques have been proven successful in reducing the recovery threshold for this task. One approach that is also very efficient in computation time is called *Rook Codes*. I also present a recent lower bound proof that says that any Rook Code for batch matrix multiplication must have a recovery threshold of at least $\omega(n)$ which was recently discovered by my collaborators and myself. Notably, we employ techniques from Additive Combinatorics in order to prove this, which may be of further interest. Moreover, we show a Rook Code that achieves a recovery threshold of $n^{1+o(1)}$, establishing a near-optimal answer to the fault tolerance of this coding scheme.

Pedro Soto
University of Oxford
Pedro.Soto@maths.ox.ac.uk

MS44

Positive Del Pezzo Geometry

Real, complex, and tropical algebraic geometry join forces in a new branch of mathematical physics called positive geometry. We develop the positive geometry of del Pezzo surfaces and their moduli spaces, viewed as very affine varieties. Their connected components are positive geometries derived from highly symmetric polytopes. We study their canonical forms and scattering amplitudes, and we solve the likelihood equations. This is work in progress with Nick Early, Marta Panizzut, Bernd Sturmfels and Claudia Yun.

Geiger Alheydis
MPI Leipzig
alheydis.geiger@mis.mpg.de

Alheydis Geiger
University of Tuebingen
alheydis.geiger@mis.mpg.de

MS44

Lines on Singular Cubic Fourfolds

In this talk, we study degenerations of the variety of lines on a cubic fourfold. The question is how the variety of lines degenerates if the fourfold degenerates. We investigate the combinatorics, the components and the singularities. This is joint work with Angel Rios Ortiz.

Christian Lehn
Technical University Chemnitz
christian.lehn@mathematik.tu-chemnitz.de

MS44

Extending Real Enumerative Geometry to Arbitrary Fields

There are 27 lines on a smooth cubic surface over $\mathbb{C}$, but there can be 3, 7, 15, or 27 real lines on a smooth cubic surface over $\mathbb{R}$. However, there are always 3 more hyperbolic lines than elliptic lines on such cubic surfaces. The separation of lines into hyperbolic and elliptic types constitutes a ”signed count”, which is a central theme in real enumerative geometry. In this talk, I will discuss ”signed counts” for various enumerative problems over arbitrary fields and introduce the $\mathbb{A}^1$-enumerative geometry program. Some of the results will be my own, but I will also cover examples due to Kass–Wickelgren, Pauli, and others. To conclude, I will discuss open questions and directions in $\mathbb{A}^1$-enumerative geometry.

Stephen McKean
Harvard University
smckean@math.harvard.edu

MS44

Real Plane Hurwitz Numbers

The classical Hurwitz numbers count the amount of simple branched coverings, of a fixed degree, from curves of fixed genus with a fixed branch locus up to isomorphism. We say that a branched covering is real if the domain curve has an involution compatible with the complex conjugation on the Riemann sphere. Analogously, plane Hurwitz numbers count the number of simple branched coverings that are a linear projections from a plane curve. This number is only known for plane curves of degree 3 and 4, and it is 40 and 120 respectively. The real plane Hurwitz numbers count the number of plane branched coverings that are real. We compute these numbers for degree 3 and 4. In the first case, the real plane Hurwitz number is 8. For degree 4, the real Hurwitz number can be 8,16,32,64,120 or 24. The results to be presented in the talk have been achieved jointly with D. Agostini, H. Markwig, C. Nollau, V. Schleis, and B. Sturmfels.

Javier Sendra-Arranz
MPI Leipzig
javier.sendra@mis.mpg.de

MS45

Locally Positive Semidefinite Matrices and Hyperbolic Polynomials

A matrix is k-locally positive semidefinite (PSD) if all of its $k \times k$ minors are positive semidefinite. I will describe some results and open questions on approximation of the cone of PSD matrices by k-locally PSD matrices and eigenvalues of k-locally PSD matrices. This will naturally lead to hyperbolic polynomials which can be expressed as linear combinations of $k \times k$-minors of a matrix. I will present some results that generalize classical linear algebra inequalities (e.g. Hadamard’s inequality) and present more open questions.

Greg Blekherman
Georgia Institute of Technology
gblekherman3@gatech.edu

MS45

A Moment Theoretic Approach to Estimate the Cardinality of Certain Algebraic Varieties

For $n \in \mathbb{N}$, we consider the algebraic variety $\mathcal{V}$ obtained by intersecting $n+1$ algebraic curves of degree n in $\mathbb{R}^2$, when the leading terms of the associated bivariate polynomials are all different. We provide a new proof, based on the Flat Extension Theorem from the theory of truncated moment problems, that the cardinality of $\mathcal{V}$ cannot exceed $\binom{n+1}{2}$. In some instances, this provides a slightly better estimate than the one given by Bézout's Theorem. Our main result contributes to the growing literature on the interplay between linear algebra, operator theory, and real algebraic geometry. The talk is based on joint work with Seonguk Yoo; a research paper with a homonymous title has appeared in *New York J. Math.* 28(2022) 357366.

Raul E. Curto
Department of Mathematics
The University of Iowa
raul-curto@uiowa.edu

MS45

Separating Cones for the SOS and PSD Cones

The cone $\mathcal{P}_{n+1,2d}$ of all positive semidefinite (PSD) real forms in $n+1$ ($n \geq 1$) variables of degree $2d$ ($d \geq 1$) contains the cone $\Sigma_{n+1,2d}$ of all real forms in $n+1$ variables of degree $2d$ that are representable as finite sums of squares (SOS) of real forms in $n+1$ variables of half degree d. In 1888, Hilbert proved that $\Sigma_{n+1,2d} = \mathcal{P}_{n+1,2d}$ exactly in the *Hilbert cases* $n+1=2$ or $2d=2$ or $(n+1,2d)=(3,4)$. In particular, for showing $\Sigma_{n+1,2d} \subsetneq \mathcal{P}_{n+1,2d}$ in any non-Hilbert case, he firstly verifies the assertion in the *basic non-Hilbert cases* $(4,4)$ and $(3,6)$. Secondly, he generalizes these findings to any non-Hilbert case by an argument that allows him to increase the number of variables and the even degree while preserving the PSD-not-SOS property.
In my talk, I will construct a filtration of intermediate cones between the SOS and PSD cones along a filtration of irreducible projective superior varieties of the Veronese variety. Then I will investigate this cone filtration for proper inclusions. Following the spirit of Hilbert, I will particularly determine all separating cones for the SOS and PSD cones in the non-Hilbert cases $(n+1,4)_{n\geq 3}$ and $(n+1,6)_{n\geq 2}$.

Sarah T. Hess
Universität Konstanz
sarah.hess@uni-konstanz.de

Salma Kuhlmann
University of Konstanz, Germany
salma.kuhlmann@uni-konstanz.de

Charu Goel
Indian Institute of Information Technology
India
charugoel@iiitn.ac.in

MS45

The Truncated Moment Problem on Some Polynomial and Rational Plane Curves

Given a finite d-dimensional real multisequence β indexed by monomials in d variables of total degree k and a closed set K of $\mathbb{R}^d$, the truncated moment problem (TMP) on K asks to characterize the existence of a positive Borel measure μ on $\mathbb{R}^d$ with support in K such that the elements of β are the moments of μ. In the talk I will present a reduction to the univariate setting technique that can be efficiently used on bivariate sequences with a moment matrix satisfying a column relation of the form $y=q(x)$, $q(x)\in\mathbb{R}[x]$, or $yx^{\ell}=1$, $\ell\in\mathbb{N}$. For $\deg q<3$ or $\ell<2$ this leads to alternative solutions to the TMP on quadratic curves, while for $\deg g \geq 3$ or $\ell \geq 2$ one gets a solution to the TMP based on the size of moment matrix extensions, which is $\deg q - 1$ or $\ell+1$ and improves previous bounds, quadratic in the degrees of the sequence and the polynomial determining a curve. This approach also gives an optimal bound on the number of atoms in a minimal representing measure and translates the problem into a positive semidefinite matrix completion problem of smaller size.

Aljaz Zalar
University of Ljubljana
aljaz.zalar@fri.uni-lj.si

MS46

Tropical Logistic Regression on the Space of Phylogenetic Trees

A phylogenetic tree is a representation of the evolutionary history between species. Tree leaves are labelled with current species, and internal nodes representing ancestral species are unlabelled. Recent technological advancements in genetics and genomics have led to cheap and fast genome data generation. This, in turn, has paved the way for the development of *phylogenomics*, a new field that applies tools in phylogenetics to conduct comparative analyses on genome data. Our goal is to develop statistical methods over the space of phylogenetic trees, which coincides with the ultrametric space and conforms to spaces from *tropical geometry*. We have developed the tropical logistic regression model, which classifies sampled gene trees into classes characterized by some species tree.

George Aliatimis
Lancaster University
g.aliatimis@lancaster.ac.uk

MS46

Multiparameter Persistence for Molecular Biology

Single-parameter persistent homology the flagship tool in topological data analysis has witnessed a wide range of successful applications in the biological sciences in the last decade. Multiparameter persistent homology is a natural generalisation allowing for higher-order analysis of more complex phenomena including time-varying data. In this talk, we demonstrate some applications of multiparameter persistent homology to spatial data in biology.

Katherine Benjamin
University of Oxford
katherine.benjamin@maths.ox.ac.uk

MS46

Invariants of Level-1 Phylogenetic Networks

We study a family of ideals associated with phylogenetic networks under the Cavendar-Farris-Neyman (CFN) model. Roughly, these ideals are used to infer the evolutionary history of a collection of species. In 2006, Sturmfels and Sullivant showed that when the underlying graph is a tree, the ideal is toric, and they give a full combinatorial description of a Grobner basis for the ideal. The story is not over, however. Recently, there has been a push to study phylogenetic networks where the underlying graph may not be a tree allowing us to describe more complicated evolutionary behavior such as hybridization and horizontal gene transfer. We will analyze the situation where these behaviors are sufficiently sparse in the network. In this case, we provide a full combinatorial description of the quadratics in the ideal while also showing the ideal is quadratically generated when there are no cycles of length greater than 8.

Joseph Cummings
University of Notre Dame
josephcummings03@gmail.com

Benjamin Hollering
Max Planck Institute
benjamin.hollering@mis.mpg.de

Christopher Manon
University of Kentucky
chris.manon@gmail.com

MS46

Quasi-Toric Differential Inclusions

Toric differential inclusions play a pivotal role in providing a rigorous interpretation of the connection between weak reversibility and the persistence of mass-action systems and polynomial dynamical systems. We introduce the notion of quasi-toric differential inclusions, which are strongly related to toric differential inclusions, but have a much simpler geometric structure. We show that every toric differential inclusion can be embedded into a quasi-toric differential inclusion and that every quasi-toric differential inclusion can be embedded into a toric differential inclusion. In particular, this implies that weakly reversible dynamical systems can be embedded into quasi-toric differential inclusions.

Abhishek Deshpande
IIIT Hyderabad
deshabhi123@gmail.com

Gheorghe Craciun
Department of Mathematics, University of
Wisconsin-Madison
craciun@wisc.edu

Hyejin Jenny Yeon
Department of Mathematics
University of Wisconsin-Madison
hyeon2@wisc.edu

MS47

Tensor Eigenvectors: a Geometric and An Algorithmic Approach

The applications of tensor spectral theory range from hypergraph theory to quantum physics, from dynamical systems to polynomial optimization, from signal processing to medical imaging. We will focus on tensor eigenvectors and their configurations. Since the eigenvector property is preserved under scalar multiplication, it is natural to regard eigenvectors as points in the projective space, and talk about eigenpoints. From the point of view of defining equations, it turns out that eigenpoint schemes are particular standard determinantal schemes. In collaboration with F. Galuppi and L. Venturello we characterized their determinantal equations. Such a result allows to design two algorithms: the first one checks if a tuple of homogeneous polynomials is the tuple of determinantal equations of an eigenscheme; the second one checks whether, given a set of points in the projective space, there exists a tensor whose eigenscheme contains the given set. If the answer is positive, it explicitly reconstructs one such tensor. Finally, we will characterize geometrically plane eigenschemes, by using classical topics like Laguerre nets of curves. Concerning higher dimensions, we will report on a joint result in collaboration with R. M. Mir-Roig, asserting that a general eigenscheme is the complete intersection of two suitable smooth determinantal curves on a smooth determinantal surface. Moreover, the converse result holds in the projective 3-space.

Valentina Beorchia
University of Trieste
beorchia@units.it

MS47

Jordan Decompositions of Tensors

We expand on an idea of Vinberg to take a tensor space and the natural Lie algebra which acts on it and embed them into an auxiliary algebra. Viewed as endomorphisms of this algebra we associate adjoint operators to tensors. We show that the group actions on the tensor space and on the adjoint operators are consistent, which endows the tensor with a Jordan decomposition. We utilize aspects of the Jordan decomposition to study orbit separation and classification in examples that are relevant for quantum information.

Luke Oeding
Auburn University
oeding@auburn.edu

Frédéric Holweck
University of Technology Belfort-Montbeliard, France
frederic.holweck@utbm.fr

MS47

On Minimal Schemes Evincing Generalized Decompositions

Finding zero-dimensional schemes of minimal length apolar to a given form F is a critical task both from theoretical and computational perspectives. In geometrical terms, this amounts to computing the cactus rank of F, which is in general a huge and often intractable problem. However, such minimal schemes are known to evince a generalized additive decomposition (GAD) of an extension of F, which motivates the study of these objects. In this talk, we will present certain families of GADs arising from a given form, and investigate some algebraic properties of the schemes they evince. Besides, we discuss the practical difficulty of detecting the best GADs, namely those evincing schemes of minimal length. This is joint work with A. Bernardi and A. Oneto.

Daniele Taufer
KU Leuven
daniele.taufer@gmail.com

MS47

Abstract Cone Systems

An Abstract Operator Systems (AOS) is a collection of a proper convex cones inside the vector space of square matrices of dimension s tensored with a vector field V, for all $s \in \mathbb{N}$. There are many examples of interesting AOS, in particular when V is also a matrix space and we fix the cone of positive semidefinite matrices on the first level. Well-studied examples are the operator system of separable matrices (arising from the *minimal* tensor product), positive simidefinite matrices, and block-positive matrices (from the *maximal* tensor product). In the higher levels, the interaction between the positive cone and the tensor product becomes particularly insightful. We propose a generalized version of AOS, called the Astract Cone System (ACS). We no longer restrict to matrix spaces (and their positive semidefinite cones), but instead look at tensor products of V with arbitrary finitedimensional vector spaces with involution. We reprove the most important theorems about AOS in the general case: the existence of minimal and maximal ACS, the existence of a finite dimensional realization as a concrete cone system, and that free dual of a finitely realizable ACS is finitely generated. This generalization not only sheds a new light on AOS and allows us to define them in a coordinate free way, it also allows to rephrase recent studies on entanglement between convex cones as ACS, offering a new toolbox and perspective.

Mirte van der Eyden, Tim Netzer
University of Innsbruck
mirte.van-der-eyden@uibk.ac.at, tim.netzer@uibk.ac.at

Gemma De les Coves
Universität Innsbruck, Austria
gemma.delascuevas@uibk.ac.at

MS48
Nullstellenstsze, Nonlocal Games, and State Dependent Contextuality

This talk investigates a link between non-commutative (NC) Nullstellenstze and nonlocal games. We'll begin by showing a general Nullstellenstze-based characterization of nonlocal games with perfect commuting operator strategies. We'll then use this characterization to discuss several well-studied families of nonlocal games, including XOR games, linear systems games, and synchronous games. Time permitting, we'll also discuss some open questions raised by this approach, and how similar techniques could be used more generally to study state-dependent contextuality questions. This talk is based on joint work with J. William Helton and Igor Klep. Arxiv number: 2111.14928.

Adam Bene Watts
Massachusetts Institute of Technology
Cambridge, MA, USA
adam.benewatts1@uwaterloo.ca

J.William Helton
University of California, San Diego
Math Dept.
helton@math.ucsd.edu

Igor Klep
University of Ljubljana, Department of Mathematics
Slovenia
igor.klep@fmf.uni-lj.si

MS48
Gibbs Manifolds

Gibbs manifolds are images of affine spaces of symmetric matrices under the exponential map. They arise in applications such as optimization, statistics and quantum physics, where they extend the ubiquitous role of toric geometry. The Gibbs variety is the zero locus of all polynomials that vanish on the Gibbs manifold. In this talk we will discuss the relevance of Gibbs manifolds to applications and various properties of Gibbs varieties, for instance that in the generic case they are low-dimensional, irreducible and unirational.

Dmitrii Pavlov
Max-Planck-Institute for Mathematics in the Sciences
Leipzig, Germany
dmitrii.pavlov@mis.mpg.de

Bernd Sturmfels
MPI Leipzig and UC Berkeley
bernd@mis.mpg.de

Simon Telen
MPI Leipzig
simon.telen@mis.mpg.de

MS48
Unitary Property Testing Lower Bounds by Polynomials

Quantum query complexity is a fundamental model in quantum computation, which captures known quantum algorithms such as Grover's search algorithm, and also enables rigorous comparison between classical and quantum models of computation. The polynomial method has become one of the main paradigms for proving lower bounds on quantum query complexity. In this work, we study unitary property testing setting, which generalizes the standard quantum query complexity model and captures "inherently quantum" problems that appear to have no classical analogue. Characterizing the query complexity of these problems requires new algorithmic techniques and lower bound methods. We prove a generalized polynomial method for analyzing the complexity of unitary property testing problems and apply this method on new problems such as unitary recurrence time, approximate dimension counting, and estimating the entanglement entropy. We highlight the use of results from invariant theory as important tools for applying the generalized polynomial method. Finally, we present a possible approach towards an oracle spearation of QMA and QMA(2), which is a long-standing question in quantum complexity theory.

Adrian She
University of Toronto
Toronto, Canad
adrian.she@mail.utoronto.ca

MS48
Tensor Parameters and Quantum Entanglement

In quantum theory, tensors over the complex numbers represent pure states of systems composed of several parts. The fundamental problem of entanglement transformations is to decide whether there is exists a transformation between a given pair of states by a sequence of local measurements on the subsystems which may depend on previous measurement results. In quantum Shannon theory, we ask whether the transformation is possible between many copies of the states, represented by tensor powers of the tensors, either exactly or approximately or with a given probability. One of the variants of this question is equivalent to asymptotic tensor restriction. We say that an order-k tensor s asymptotically restricts to t if $(A_1 \otimes \cdots \otimes A_k)s^{\otimes n} = t^{\otimes n}$ for large n and suitable linear maps $A_1, \ldots, A_k$. Any tensor parameter that is monotone under restriction and multiplicative under the tensor product provides a necessary condition for asymptotic restriction, and analogous quantities can be defined for entanglement transformations as well. The aim of this talk is to explain some of the connections between these problems.

Péter Vrana
Budapest University of Technology and Economics
vranap@math.bme.hu

MS49

Certified Approximations to Pairs of Real Curves in the Plane

I will address the problem of computing a topologically correct piecewise-linear approximation to a pair of real smooth implicit curves in the plane. The most substantial challenge in this problem is to guarantee that the intersection of the approximations correctly approximates the intersection of the curves. I will discuss a new algorithm, which is based on the Plantinga-Vegter subdivision scheme for correctly approximating individual curves. Our algorithm introduces a new and simple predicate to their subdivision scheme. We prove that this predicate is enough to guarantee the topological correctness of our resulting pair of approximations, and that the algorithm remains efficient in practice.

Michael A. Burr, Michael Byrd
Clemson University
burr2@clemson.edu, mbyrd6@clemson.edu

MS49

Isolating Clusters of Zeros of Analytic Systems Using Arbitrary-degree Inflation

The zero cluster isolation problem seeks to construct two regions that contain a cluster of zeros for a given system of analytic functions, with the smaller region tightly containing the cluster and the larger region separating it from other zeros of the system. We introduce the counterintuitive but certified approach of using the inflation method to solve this problem. We will provide an algorithmic overview of the method and illustrate cases where it can be applied. This is based on a joint work with Michael Burr and Anton Leykin.

Kisun Lee
University of California, San Diego, U.S.
kil004@ucsd.edu

MS49

Answering Efficiently Connectivity Queries on Real Algebraic Space Curves

Using the notion of roadmaps, one can reduce connectivity queries in real algebraic sets of arbitrary dimension to such queries in real algebraic curves, making this a topical problem in computational real algebraic geometry. I will present an algorithm for solving the latter problem. Our approach avoids the determination of the complete topology of the curve, which allows significant speed-ups with respect to the state-of-the-art. This is joint work with Md Nazrul Islam and Adrien Poteaux.

Rémi Prébet
LIP6, Sorbonne University and French Ntl Ctr Sci Research
remi.prebet@lip6.fr

MS49

Certifying Zeros of Polynomial Systems Using Interval Arithmetic

The field of computational algebraic geometry is often associated with symbolic computations based on Grbner bases, but over the last thirty years numerical algebraic geometry emerged as an alternative. Based on the algorithmic framework homotopy continuation it solves problems that are infeasible with symbolic methods. Yet, without certification numerical methods cant be used for proofs, which restricts their use in pure mathematics. We discuss how to combine interval arithmetic and Krawczyks method with numerical algebraic geometry to rigorously certify solutions to square systems of polynomial equations. We present a fast implementation, making certification the default option, and enabling the extensive use of numerical methods for rigorous proofs.

Kemal Rose
Max-Planck Institute for Mathematics in the Sciences
kemal.rose@mis.mpg.de

MS50

Homological Approximations in Persistence Theory

Multiparameter persistence modules do not admit a complete discrete invariant. One therefore tries to approximate such a module by a more manageable class of modules. Using that approach we define a class of invariants for persistence modules based on ideas from homological algebra. This is a report on joint work with Benjamin Blanchette and Eric Hanson.

Thomas Brüstle
Bishop's University and University of Sherbrooke
Thomas.Brustle@usherbrooke.ca

MS50

On Interval Resolutions of Persistence Modules

In topological data analysis, one-parameter persistent homology can be used to describe the topological features of data in a multiscale way via the persistence barcode, which can be formalized as a decomposition of a persistence module into interval representations. Multi-parameter persistence modules, however, do not necessarily decompose into intervals and thus (together with other reasons) are complicated to describe. In this talk I will discuss some recent results concerning the use of relative homological algebra with respect to intervals in the study of multi-parameter persistence modules and more generally persistence modules over posets. In particular I will discuss some results concerning the properties and computation of the "interval resolution global dimension" of posets, and provide examples of posets with small interval resolution global dimension. I will also talk about some properties of "interval covers" and "interval resolution" of persistence modules and their relationships with other invariants. This talk is based on joint works with Hideto Asashiba, Ken Nakashima, and

Michio Yoshiwaki, and on work in preparation with Toshitaka Aoki and Shunsuke Tada.

Emerson Escolar
Kobe University
e.g.escolar@people.kobe-u.ac.jp

MS50

Efficient Two-Parameter Persistence Computation via Cohomology

Clearing is a simple but effective optimization for the standard algorithm of persistent homology, which dramatically improves the speed and scalability of persistent homology computations for Vietoris–Rips filtrations. Due to the quick growth of the boundary matrices of a Vietoris–Rips filtration with increasing dimension, clearing is only effective when used in conjunction with a dual (cohomological) variant of the standard algorithm. This approach has not previously been applied successfully to the computation of two-parameter persistent homology. We introduce a cohomological algorithm for computing minimal free resolutions of two-parameter persistent homology that allows for clearing. To derive our algorithm, we extend the duality principles which underlie the one-parameter approach to the two-parameter setting. We provide an implementation and report experimental run times for function-Rips filtrations. Our method is faster than the current state-of-the-art by a factor of up to 20.

Ulrich Bauer, Fabian Lenzen
Technische Universität München, Germany
mail@ulrich-bauer.org, fabian.lenzen@tum.de

Michael Lesnick
University at Albany, U.S.
mlesnick@albany.edu

MS50

The Volume Noise System for Multi-parameter Persistence

Noise systems provide a framework for defining metrics on multi-parameter persistence modules, by defining what is to be considered small (noise) in an axiomatic way. In this talk I will first review how noise system based distances account for well known distances in TDA such as the interleaving distance in multi-parameter persistence and Wasserstein metrics (in the one parameter case). The focus will be then on exploring a new distance between persistence modules, defined by the so called volume noise system. Distances between two persistence modules, with respect to volume noise, depend on the geometry of the support of the modules. Although such distances are in general hard to compute we can use them to define a stable invariant of multi-persistence modules called stable rank. We will see that stable rank with respect to volume noise are in general not additive and discuss an additive alternative.

Martina Scolamiero
KTH Stockholm
scola@kth.se

René Corbet
KTH Stockholm, Sweden
corbet@kth.se

MS51

Multigraded Regularity of Curves

The syzygies of projective curves are fairly well understood for instance, an influential theorem of Gruson, Lazarsfeld, and Peskine gives optimal bounds on their regularity. There has been a flurry of activity in the past two decades centered around generalizing work on syzygies to the toric setting. I will discuss work that lifts machinery for understanding syzygies of projective curves to obtain a bound on the multigraded regularity of a curve in a product of projective spaces.

John Cobb
University of Wisconsin-Madison
jcobb2@math.wisc.edu

MS51

Castelnuovo-Mumford Regularity of Projective Monomial Curves via Sumset

Given $A = \{a_0, \ldots, a_{n-1}\}$ a finite set of $n \geq 4$ non-negative integers that we will assume to be in normal form, i.e., such that $0 = a_0 < a_1 < \cdots < a_{n-1} = d$ and relatively prime, the s-fold sumset of A is the set sA of integers obtained as the sum of s elements in A. On the other hand, given an infinite field k, one can associate to A the projective monomial curve C_A parametrized by A:

$$C_A = \{(v^d : u^{a_1}v^{d-a_1} : \cdots : u^{a_{n-2}}v^{d-a_{n-2}} : u^d)\}$$

where $(u : v)$ covers the whole projective line over k. In this talk, we will focus on the relation between the Castelnuovo-Mumford regularity of C_A and the behaviour of the sumsets sA and show how this provides a nice interplay between Commutative Algebra and Additive Number Theory.

Philippe Gimenez, Mario González-Sánchez
Universidad de Valladolid
pgimenez@uva.es, mario.gonzalez.sanchez@uva.es

MS51

Characterizing Multigraded Regularity on Products of Projective Spaces

Motivated by toric geometry, Maclagan-Smith defined the multigraded Castelnuovo-Mumford regularity for sheaves on a simplicial toric variety. While this definition reduces to the usual definition on a projective space, other descriptions of regularity in terms of the Betti numbers, local cohomology, or resolutions of truncations of the corresponding graded module proven by Eisenbud and Goto are no longer equivalent. I will discuss recent joint work with Lauren Cranton Heller and Juliette Bruce on generalizing Eisenbud-Goto's conditions to the "easiest difficult" case, namely products of projective spaces, and our hopes and dreams for how to do the same for other toric varieties.

Mahrud Sayrafi
University of Minnesota
mahrud@umn.ed

MS52

An E-Infinity Structure on the Matroid Grassmannian

The matroid Grassmannian is the space of oriented matroids. 30 years ago MacPherson showed us that understanding the homotopy type of this space can have significant implications in manifold topology. In some easy cases, the matroid Grassmannian is homotopy equivalent to the ordinary real Grassmannian, but in most cases we have no idea whether or not they are equivalent. This is known as MacPherson's conjecture. I'll show that one of the important homotopical structures of the ordinary Grassmannians has an analogue on the matroid Grassmannian, namely the direct sum monoidal product that is commutative up to all higher homotopies.

Jeffrey H. Giansiracusa
Swansea University
jeffrey.giansiracusa@durham.ac.uk

MS52

Computing Tropical Median Consensus Trees

In computational biology, a phylogenetic tree is the standard model for organizing ancestral relations among species or individual organisms. Since many different methods are known to construct various trees from one fixed data set, there is a need for algorithms to find the common ground. Such an algorithm gives rise to some "consensus tree", which describes where the given trees agree. In this talk we will present a new procedure for computing consensus trees, crucially based on methods of tropical combinatorics. We will emphasize the computational aspects of our method.

Andrei Comaneci
Technische Universität Berlin
comaneci@math.tu-berlin.de

Michael Joswig
Technische Universität Berlin, Germany
joswig@math.tu-berlin.de

MS52

Separation Theorems in Signed Tropical Convexities

The max-plus semifield can be equipped with a natural notion of convexity called the "tropical convexity". This convexity has many similarities with the standard convexity over the non-negative real numbers. However, the restriction to non-negative numbers implies that some properties of classical objects are lost in the tropical setting. For instance, two generic tropical lines in a real tropical plane may not intersect. In order to avoid this problem, one can work with signed tropical numbers. Recently, a definition of convexity over the signed tropical numbers was proposed by Loho and Vgh. This notion, called the TO-convexity, is based on a multi-valued addition of signed tropical numbers. In this talk, I will present a new version of signed tropical convexity, the TC-convexity, and compare it with the TO-convexity. The TC-convexity is based on a non-commutative addition of signed tropical numbers, which generalizes the composition operation of signed sets that is used to define oriented matroids. Our main result is a hyperplane separation theorem stating that the TC-convex hull of finitely may points coincides with the intersection of all closed tropical half-spaces that contain these points.

Georg Loho
University of Twente
g.loho@utwente.nl

Mateusz Skomra
LAAS-CNRS, Université de Toulouse, CNRS
mateusz.skomra@laas.fr

MS52

No Self-Concordant Barrier Interior Point Method Is Strongly Polynomial

A long-standing candidate to solve Smale's ninth problem of solving linear programming in strongly polynomial complexity (*i.e.* polynomial in the number of inputs instead of their bitsize) has been the theory of self-concordant barrier interior point methods (IPMs). These follow the *central path*, a curve in the interior of the feasible set, up to an approximate solution of the problem. It was shown in [Allamigeon, Benchimol, Gaubert and Joswig, SIAGA, 2018] that IPMs based on the logarithmic barrier are not strongly polynomial. The authors studied the central paths of parametric families of linear programs by looking at their *tropicalization*, *i.e.* the limit of their log-image, which is a piecewise linear curve called the tropical central path. We present our contribution showing that *none* of the self-concordant barrier IPMs are strongly polynomial. To achieve this, we show that IPMs draw polygonal curves in a multiplicative neighborhood of the central path whose log-limit coincides with the tropical central path, independently of the barrier. It entails that IPMs must do at least as many iterations as there are segments composing the tropical central path. We provide an explicit parametric linear program that falls in the same class as the Klee–Minty counterexample, *i.e.* whose feasible set is an n-dimensional combinatorial cube. Its tropical central path is composed of $2^n - 1$ segments, thus breaking strong polynomiality.

Xavier Allamigeon
INRIA and CMAP, Ecole Polytechnique, CNRS
xavier.allamigeon@inria.fr

Stephane Gaubert
INRIA and CMAP, Ecole Polytechnique
stephane.gaubert@inria.fr

Nicolas Vandame
CMAP, École polytechnique, CNRS, Institut
polytechnique de P
nicolas.vandame@polytechnique.edu

MS53

Faster Beta Weil Pairing on BLS Pairing Friendly Curves with Odd Embedding Degree

Since the advent of pairing-based cryptography, various optimization methods that increase the speed of pairing computations have been exploited, as well as new types of pairings. In this work we proposed new formulas for the Beta-Weil pairing on curves with odd embedding degree by eliminating denominators and exponents during the computation of the Beta-Weil pairing. These formulas are suitable for the parallel computation for the Beta-Weil pairing on curves with odd embedding degree which involve vertical line functions useful for sparse multiplications. For computations we used Millers algorithm combined with storage and multifunction methods. Applying our framework to BLS-27, BLS-15 and BLS-9 curves at respectively the 256 bit, the 192 bit and the 128 bit security level, we obtain faster Beta-Weil pairings than the previous state-of-the-art constructions.

Laurian Azebaze Guimagang
University of Yaounde 1, Cameroon
azebazelaurian@yahoo.fr

MS53

Swiftec: Shalluevan De Woestijne Indifferentiable Function To Elliptic Curves

Hashing arbitrary values to points on an elliptic curve is a required step in many cryptographic constructions, and a number of techniques have been proposed to do so over the years. One of the first ones was due to Shallue and van de Woestijne (ANTS-VII), and it had the interesting property of mapping essentially any finite field to any elliptic curve over that field. It did not, however, have the desirable property of being indifferentiable from a random oracle when composed with a random oracle to the base field. Various approaches have since been considered to overcome this limitation, but despite being successful they all have the drawback of being twice as expensive to compute, requiring two field exponentiations. In this work, we revisit this long-standing open problem, and observe that the SW map actually fits in a one-parameter family of encodings, where treating the parameter as a second input results in a map to the curve that is indifferentiable. Moreover, on a very large class of curves, the one-parameter family admits a rational parametrization, which lets us compute the map at almost the same cost as the original, and finally achieve indifferentiable hashing to most curves with a single exponentiation.

Jorge Chavez Saab
CINVESTAV-IPN, Technology Innovation Institute, Mexico
jorgechavezsaab@gmail.com

Mehdi Tibouchi
NTT, Japan
mehdi.tibouchi@normalesup.org

Francisco Rodriguez-Henriquez
Technology Innovation Institute
francisco.rodriguez@tii.ae

MS53

Introduction on Elliptic Curves and Pairings in Cryptography

Elliptic curves over large prime fields are widely deployed in non-quantum public-key cryptography. Since 2001, pairing-friendly curves allow to design new cryptosystems (identity-based encryption and short signatures are classical examples). These pairing-friendly curves are equipped with a bilinear map efficiently computable: the Tate or the Weil pairing. Variants of the Tate pairing are usually the most efficient in common cryptographic contexts. More recently in the context of proof systems, new needs of elliptic curves arise. This mini-symposium focuses on pairing-friendly elliptic curves revisited with these new applications in mind: finding new pairing-friendly curves, finding chains or cycles of pairing-friendly elliptic curves, hashing to the group of points on a curve, improving the pairing computation in different contexts, improving the group operations (testing membership of a subgroup of the curve, or mapping a point to a specific subgroup).

Aurore Guillevic
Inria Nancy Grand Est
aurore.guillevic@inria.fr

MS53

Subgroup Membership Testing on Elliptic Curves via the Tate Pairing

In my talk I will explain how to guarantee the membership of a point in the prime-order subgroup of an elliptic curve (over a finite field) satisfying some moderate conditions. For this purpose, we will apply the Tate pairing on the curve, however it is not required to be pairing-friendly. Whenever the cofactor is small, the new subgroup test is much more efficient than other known ones, because it needs to compute at most two n-th power residue symbols (with small n) in the basic field. More precisely, the running time of the test is (sub-)quadratic in the bit length of the field size, which is comparable with the Decaf-style technique. The test is in particular relevant for most real-world twisted Edwards curves.

Dimitri Koshelev
ENS Lyon, France
dimitri.koshelev@gmail.com

MS54

Constructing Moderate-Density Parity-Check Codes from Projective Bundles

Moderate-Density Parity-Check (MDPC) codes were introduced as an extension of low-density parity-check (LDPC) codes and are of high interest in cryptographic applications. In this talk we present a new construction of a family of MDPC codes using projective bundles in a Desarguesian projective plane. In a projective plane of order q such a bundle consists of $q^2 + q + 1$ ovals that are mutually intersecting in a unique point. We define a parity check matrix as the incidence matrix between the points of a projective plane and the lines together with the ovals of a projective bundle. Furthermore, we completely determine their dimension and minimum distance for both q even and odd. In addition, we observe that we can design these codes to possess a quasi-cyclic structure of index 2.

Jessica Bariffi
German Aerospace Center
jessica.bariffi@dlr.de

Sam Mattheus
University of California, San Diego
smattheus@ucsd.edu

Alessandro Neri
Ghent University
alessandro.neri@ugent.be

Joachim Rosenthal
Institut für Mathematik
Universität Zürich
rosenthal@math.uzh.ch

MS54

On the Exceptionality of Rational APN Functions

Almost perfect nonlinear (APN) functions, and the exceptional ones in particular, have been also investigated in connection with algebraic varieties over finite fields, whose degree strictly depends on the the degree of the corresponding polynomial. In this direction, non-existence results were obtained by means of estimates on the number of $\mathbb{F}_q$-rational points of such varieties, as Hasse-Weil or Lang-Weil bounds, which can be applied only if the degree of the polynomial under investigation is small enough. On the one hand, using such a machinery non-existence results were obtained only in small-degree regime or of so-called exceptional APN functions. On the other hand, not all the examples of APN functions are described in the literature by polynomials. In fact, the inverse map $x \mapsto x^{-1}$ is known to be APN on $\mathbb{F}_{2^n}$ with n odd, and thus it is also exceptional. Such a map, seen as a polynomial function, has large degree (the function coincides with x^{2^n-2}) and thus the previous machinery does not apply. Inspired by this example, we start the investigation of APN functions which can be represented as rational functions and we provide non-existence results exploiting the connection between these functions and specific algebraic varieties over finite fields. This approach allows to classify families of functions when previous approaches cannot be applied.

Francesco Ghiandoni
Univeristà degli studi di Firenze
francesco.ghiandoni@unifi.it

MS54
Relative Hulls and Quantum Codes

The relative hull of a code C_1 with respect to another code C_2 is the intersection $C_1 \cap C_2^{\perp}$. We prove that the dimension of the relative hull can always be repeatedly reduced by one by replacing any of the two codes with an equivalent one. Specifically, we show how to construct an equivalent code C_1' of C_1 such that the dimension of $C_1' \cap C_2^{\perp}$ is one less than the dimension of $C_1 \cap C_2^{\perp}$. These results apply to hulls taken with respect to the e-Galois inner product, which has as special cases both the Euclidean and Hermitian inner products. We study the consequences of the relative hull properties on quantum codes constructed via CSS construction. This is joint work with S. Anderson (University of St. Thomas), E. Camps-Moreno (National Polytechnic Institute of Mexico), G. Matthews (Virginia Tech), D. Ruano (Universidad de Valladolid), and I. Soprunov (Cleveland State University).

Hiram H. Lopez
Cleveland State University
h.lopezvaldez@csuohio.edu

MS54
Intertwined Results in Finite Geometry and Coding Theory

It has been known for many decades that finite geometry and coding theory are related areas, and many results can be equivalently stated in the two languages; for instance, the MDS conjecture for linear codes can be described in terms of arcs in a finite projective space. The relation between finite geometry and coding theory is not just a matter of language: geometric tools have been applied in coding theory, and coding-theoretic methods have played a role in geometric problems. Recently, many researchers have pushed forward with this relation in several directions: for instance, regarding new metrics for error-correcting codes; or the construction of quantum codes from classical ones; or the application of more refined algebraic methods. The talks of the minisymposium give evidence of the recent developments in many directions, and this talk will give an overview of some old and new results in the intertwined areas of finite geometry and coding theory.

Giovanni Zini
Università degli studi di Modena e Reggio Emilia
giovanni.zini@unimore.it

MS55
Lorentzian Polynomials from Matroid Bundles

We give an introduction to Lorentzian polynomials, and discuss how they arise in the context of matroid theory.

Christopher Eur
Stanford University
Department of Mathematics
chriseur@stanford.edu

MS55
Examples of Lorentzian Polynomials in Combinatorics and Representation Theory

The purpose of this talk will be to share several families of polynomials that are either known or expected to be Lorentzian. Two important classes I will focus on are the (normalizations of) Schur polynomials and the chromatic symmetric functions of certain graphs appearing in the study of Hessenberg varieties. If time permits, I may discuss stronger conjectures involving stability. The talk will be based on joint work with June Huh, Karola Mszros, Alejandro Morales, Jesse Selover, and Avery St. Dizier.

Jacob Matherne
University of Bonn
jacobm@math.uni-bonn.de

MS55
Lorentzian Polynomials and Volume Polynomials

In 1901, Minkowski showed that the volume of a linear combination of convex bodies with non-negative coefficients gives rise to a homogeneous polynomial, the so-called volume polynomial. Starting with the Alexandrov-Fenchel inequality, there has been a lot of progress throughout the years in the study of the coefficients of volume polynomials. For example, Brndn und Huh (2019) showed that every volume polynomial is a Lorentzian polynomial, but the converse is generally not true. In this talk, using our knowledge of Lorentzian polynomials, we discuss some properties of volume polynomials and construct explicit examples of Lorentzian polynomials which cannot arise as volume polynomials.

Amelie Menges
Technical University of Dortmund
amelie.menges@math.tu-dortmund.de

MS55
Toward a Generalized Lorentzian Theory for Delta Matroids

In this talk, we explore the fractional log-concavity property of generating polynomials of delta matroids. This property is an analog to the Lorentzian [Branden-Huh19]/log-concavity [Anari-Liu-OveisGharan-Vinzant19] property of the generating polynomials of matroids. We show that multivariate generating polynomials without roots in a sector of the complex plane are fractionally log-concave. This implies the fractional log-concavity of the generating polynomials of linear delta matroids since these polynomials are Hurwitz stable a.k.a. have no roots in the right half-plane. We conjecture that all delta matroids have fractionally log-concave generating polynomials, and present preliminary evidence and findings supporting this conjecture. Based on joint works with Yeganeh Alimohammadi , Nima Anari and Kirankumar Shiragur.

Thuy-Duong Vuong
Stanford University
tdvuong@stanford.edu

MS56

Algebraic Optimization of Sequential Decision Problems

In this talk we study the optimization of the expected long-term reward in finite partially observable Markov decision processes over the set of stationary stochastic policies. In the case of deterministic observations, also known as state aggregation, the problem is equivalent to optimizing a linear objective subject to quadratic constraints. We characterize the feasible set of this problem as the intersection of a product of affine varieties of rank one matrices and a polytope. Based on this description, we obtain bounds on the number of critical points of the optimization problem. Finally, we conduct experiments in which we solve the KKT equations or the Lagrange equations over different boundary components of the feasible set, and compare the result to the theoretical bounds and to other constrained optimization methods. This talk is based on joint work with M. Garrote-Lpez, G. Montfar, J. Mller, and K. Rose.

Mareike Dressler
School of Mathematics and Statistics
University of New South Wales
m.dressler@unsw.edu.au

Marina Garrote-López
Universitat Politecnica de Catalunya
marina.garrote@upc.edu

Guido F. Montufar
UCLA
guidomontufar@gmail.com

Johannes Müller
Max Planck Institute for Mathematics in the Sciences
johannes.mueller@mis.mpg.de

Kemal Rose
Max-Planck Institute for Mathematics in the Sciences
kemal.rose@mis.mpg.de

MS56

Positivity and the Moment Problem for Noncommutative Polynomials Involving the Trace

Optimization problems involving polynomial data arise across many areas of modern science and engineering. Due to recent advances, e.g., the Lasserre sum of squares hierarchy, these can nowadays be efficiently solved using semidefinite programming. Several areas of science regularly optimize functions involving polynomial data in noncommuting variables, such as matrices or operators. For instance, control theory, quantum information theory or quantum chemistry. This talk will introduce state polynomials, i.e., polynomials in noncommuting variables and formal states of their products. The motivation behind this theory arises from the study of correlations in quantum networks. Namely, determining the maximal quantum violation of a polynomial Bell inequality for an arbitrary network can be reformulated as a state polynomial optimization problem. A state analog of Artin's solution to Hilbert's 17th problem will be proved showing that state polynomials, positive over all matrices and matricial states, are sums of squares with denominators. Somewhat surprisingly, a Krivine-Stengle Positivstellensatz fails to hold in the state polynomial setting. Nevertheless, archimedean Positivstellenstze in the spirit of Putinar and Helton-McCullough will be presented leading to a hierarchy of semidefinite relaxations converging monotonically to the optimum of a state polynomial subject to state constraints. Throughout the talk explicit examples will be presented and analyzed.

Igor Klep
University of Ljubljana, Department of Mathematics
Slovenia
igor.klep@fmf.uni-lj.si

Victor Magron
CNRS LAAS
victor.magron@laas.fr

Jurij Volcic
Drexel University
jurij.volcic@drexel.edu

Jie Wang
Academy of Mathematics and Systems Science
Chinese Academy of Sciences
wangjie212@amss.ac.cn

MS56

Germination Phenomena

Many theorems in complex analysis propagate analyticity, such as the Forelli theorem, edge-of-the-wedge theorem and so on. We give a germination theorem which allows for general analytic propagation in complete normed fields. In turn, we develop general analogs of the Forelli theorem, edge-of-the-wedge theorem, and the royal road theorem, and gain insight into the geometry of the zero sets of hyperbolic polynomials.

James Pascoe
Department of Mathematics, Drexel University
pascoej@gmail.com

MS56

Deciding Membership in the Cone of Sums of Squares plus Sums of Nonnegative Circuit Polynomials

The set of all n-variate forms over $\mathbb{R}$ of degree $2d$, which are positive semidefinite (PSD), is denoted by $P_{n,2d}$. Checking membership in $P_{n,2d}$ is a fundamental problem in real algebraic geometry and has applications in polynomial optimization. Since checking membership in $P_{n,2d}$ is in general NP-hard, one often aims for appropriate subcones instead. Two subcones, which are intensely studied in the literature, are the sums of squares (SOS) cone $\Sigma_{n,2d}$ and the sums of nonnegative circuit (SONC) forms cone $C_{n,2d}$. With semidefinite programming (SDP) and Lasserre's hierarchy, the cone $\Sigma_{n,2d}$ has proven to be a powerful tool for polynomial optimization. As an alternative, the cone $C_{n,2d}$ has gained a lot of interest in recent years with relative entropy programmy (REP) and second order cone programming (SOCP) approaches. In this talk, we study the convex hull of $\Sigma_{n,2d} \cup C_{n,2d}$, i.e. the Minkowski sum $(\Sigma{+}C)_{n,2d} := \Sigma_{n,2d}{+}C_{n,2d}$, which we call the SOS+SONC cone. Indeed, this is both a proper subcone of the PSD cone and a proper extension of the SOS and SONC cones for all cases $n \geq 3, 2d \geq 4, (n, 2d) \neq (3, 4)$. We see how membership in $(\Sigma + C)_{n,2d}$ can be checked via a combination of SDP and REP. Further, we look into Positivstellensätze for the SOS+SONC cone.

Moritz Schick
Universität Konstanz
moritz.schick@uni-konstanz.de

MS57

The Embedding Problem in Phylogenetics

In this talk, we discuss the embedding problem for Markov matrices occurring in the Strand Symmetric Models. These models capture the substitution symmetries arising from the double helix structure of the DNA. Deciding whether a Markov matrix is embeddable or not enables us to know if the observed substitution probabilities are consistent with a homogeneous continuous time substitution model. Moreover, we also discuss the embedding problem for centrosymmetric matrices, which are higher order generalizations of the matrices occurring in Strand Symmetric Models. This talk is based on a joint work with Dimitra Kosta and Jordi Roca-Lacostena.

Muhammad Ardiyansyah
Aalto University
muhammad.ardiyansyah@aalto.fi

MS57

How to 3D-reconstruct the Genome From Partially Phased Data

The 3-dimensional (3D) structure of the genome is of significant importance for many cellular processes, and it can be reconstructed from the data Hi-C matrix for haploid organisms [Oluwadare et al., An overview of methods for reconstructing 3-d chromosome and genome structures from hi-c data, Biol. Proced. Online, 2019]. However, humans, like most mammals, are diploid organisms, and this poses additional challenges. First, we will see that knowing the locations of a small amount of diploid data (partially phased data) is sufficient to ensure that there are generically finitely many possible locations for the remaining part of the data, independently of the noise level. Given such a result, I will describe a novel 3D reconstruction method (SNLC) based on semidefinite programming paired with numerical algebraic geometry and local optimization. SNLC outperforms PASTIS [Cauer et al., Inferring diploid 3D chromatin structures from Hi-C data, 19th International Workshop on Algorithms in Bioinformatics, 2019] on simulated data, under different noise levels and amounts of phased data, and when it is applied on a real dataset from mouse X chromosomes, it recovers previously known structural features.

Annachiara Korchmaros
University of Leipzig
annachiara@bioinf.uni-leipzig.de

MS57

Single Cell 3D Genome Reconstruction in the Haploid Setting Using Rigidity Theory

We study the problem of 3D genome reconstruction from contact count matrices for single cell data, and the uniqueness of such reconstructions in the setting of haploid organisms. We consider multiple models as representations of this problem, and use techniques from graph rigidity theory to determine uniqueness. Finally, we compare the 3D reconstructions for different models using semidefinite programming.

Sean Dewar
University of Bristol
sean.dewar@bristol.ac.uk

Georg Grasegger
RICAM - Linz
georg.grasegger@ricam.oeaw.ac.at

Kaie Kubjas
Aalto University
kaie.kubjas@aalto.fi

Fatemeh Mohammadi
KU Leuven
fatemehmohammadi@kuleuven.be

Anthony Nixon
Lancaster University
a.nixon@lancaster.ac.uk

MS57

When an Algebraist Meets a Crystallographer...

In this talk, I will give an overview of a paper that came out of a recent collaboration with a crystallographer, the results of which surprised both of us. The symmetries of a crystal are determined by its three-dimensional point group, and the 32 possible groups fall into one of 7 well-known crystal systems: triclinic, monoclinic, orthorhombic, tetragonal, trigonal, hexagonal, and cubic. We find that the Hasse diagram of these groups and their subgroups are built with six structural motifs, which are even or odd. Exactly 29 crystal groups, which comprise 6 of the 7 crystal systems, appear in a unique motif, and thus have a well-defined parity. In contrast, the three monoclinic crystal groups are ”ambidextrous” – they can appear in two motifs, one of each parity. There is an analogous situation in the 10 two-dimensional point groups. The simplicity of this uniform structure, and the fact that it seems to have gone unnoticed for so long, came as a surprise both of us.

Matthew Macauley
School of Mathematical & Statistical Sciences
Clemson University
macaule@clemson.edu

Maureen Julian
Virginia Tech
erie@vt.edu

MS58

Classifying Tree Topology Changes along Tropical Line Segments

The space of phylogenetic trees arises naturally in tropical geometry as the tropical Grassmannian. Tropical geometry therefore suggests a natural notion of a tropical path between two trees, given by a tropical line segment in the tropical Grassmannian. It was previously conjectured that tree topologies along such a segment change by a combinatorial operation known as Nearest Neighbor Interchange (NNI). We provide counterexamples to this conjecture, but prove that changes in tree topologies along the tropical line segment are either NNI moves or "four clade rearrangement" moves for generic trees. In addition, we show that the number of NNI moves occurring along the tropical line segment can be as large as n^2, but the average number of moves when the two endpoint trees are chosen at random is $O(n(\log n)^4)$. This is in contrast with $O(n \log n)$, the average number of NNI moves needed to transform one tree into another.

Shelby Cox
University of Michigan, Ann Arbor
spcox@umich.edu

MS58

Myths and Best Practices on Markov Bases Part 1

We look at proper ways of running Markov chains with Markov bases, while guaranteeing fiber connectivity, despite complexity, sampling, or structural constraints. We reflect on recent statistics literature on the use of Markov bases for sampling from conditional distributions, and various issues raised regarding their complexity, use and applicability in practice. We address misconceptions about Markov bases and their solutions. This is joint work with Felix Almendra-Hernandez and Sonja Petrovic.

Jesus De Loera
University of California, Davis
deloera@math.ucdavis.edu

MS58

Affine Hyperplanes and Isometry in BHV Phylogenetic Tree Space

Phylogenetic trees represent the evolutionary branching process of a set of interrelated species, such as animals, diseases, or language. As introduced in 2001 by Billera, Holmes, and Vogtmann, the BHV space of phylogenetic trees provides a piecewise Euclidean, CAT(0) metric for the moduli space of arbitrary weighted trees with a fixed leaf set. This can be used to define statistics on sets of phylogenetic trees obtained from different data sets, including different gene sequence alignments and different inference methods. However, the combinatorial complexity of BHV space, which can be most easily represented as a highly singular cube complex, impedes traditional optimization and Euclidean statistics, as the number of cubes grows exponentially in the number of leaves. Accordingly, many important geometric objects in this space are also difficult to compute, having the structure of an exponential number of locally-Euclidean cells, with combinatorial gluing properties. In this talk, I'll discuss affine hyperplanes and balls of fixed radius in BHV tree space, and how their characterization and computation can be applied to data analysis problems such as supertree contruction and compatibility testing, as well as a proof that the isometry group coincides with the isomorphism group of the underlying complex.

Gillian Grindstaff
University of California, Los Angeles
grindstaff@math.ucla.edu

MS58

Curved Markov Chain Monte Carlo for Network Learning

We present a geometrically enhanced Markov chain Monte Carlo sampler for networks based on a discrete curvature measure defined on graphs. Specifically, we incorporate the concept of graph Forman curvature into sampling procedures on both the nodes and edges of a network explicitly, via the transition probability of the Markov chain, as well as implicitly, via the target stationary distribution, which gives a novel, curved Markov chain Monte Carlo approach to learning networks. We show that integrating curvature into the sampler results in faster convergence to a wide range of network statistics demonstrated on deterministic networks drawn from real-world data.

Anthea Monod
Imperial College London
a.monod@imperial.ac.uk

Emil Saucan
ORT Braude College, Israel
semil@braude.ac.il

John Sigbeku
Imperial College London
j.sigbeku777@gmail.com

MS59

Computing Linear Sections of Varieties: Quantum Entanglement, Tensor Decompositions and Beyond

We study the problem of finding elements in the intersection of an arbitrary conic variety in $\mathbb{F}^n$ with a given linear subspace (where $\mathbb{F}$ can be the real or complex field). This problem captures a rich family of algorithmic problems under different choices of the variety. The special case of the variety consisting of rank-1 matrices already has strong connections to central problems in different areas like quantum information theory and tensor decompositions. This problem is known to be NP-hard in the worst-case, even for the variety of rank-1 matrices. Surprisingly, despite these hardness results we give efficient algorithms that solve this problem for "typical" subspaces. Here, the subspace $U \subseteq \mathbb{F}^n$ is chosen generically of a certain dimension, potentially with some generic elements of the variety contained in it. Our main algorithmic result is a polynomial time algorithm that recovers all the elements of U that lie in the variety, under some mild non-degeneracy assumptions on the variety. As corollaries, we obtain the following results: Polynomial time algorithms for generic instances of low-rank decomposition problems that go beyond tensor decompositions. Here, we recover a decomposition of the form $\sum_i v_i \otimes w_i$, where the v_i are elements of the given variety X. Polynomial time algorithms for several entangled subspaces problems in quantum entanglement.

Benjamin Lovitz
Northeastern University
benjamin.lovitz@gmail.com

MS59

Multilinear Hyperquiver Representations

We study the generalisation of quivers to directed hypergraphs. Assigning vector spaces to its nodes and multilinear maps to the its hyperedges gives a hyperquiver representation. Hyperquiver representations generalise quiver representations (where all hyperedges are edges) and tensors (where there is only one multilinear map). The singular vectors of a hyperquiver representation are a compatible assignment of vectors to the nodes. We compute the dimension and degree of the the variety of singular vectors of a hyperquiver representation. Our formula specialises to the result of Friedland and Ottaviani to count the singular vector tuples of a generic tensor, as well as to the formula of Cartwright and Sturmfels to count the eigenvectors of a generic tensor.

Tommi Muller
University of Oxford, UK
tommi.muller@maths.ox.ac.uk

Vidit Nanda
University of Oxford
nanda@maths.ox.ac.uk

Anna Seigal
Harvard University, U.S.
aseigal@seas.harvard.edu

MS59

What is the Probability That a Random Symmetric Tensor is Close to Rank-one?

We address the general problem of estimating the probability that a real symmetric tensor is close to rank-one tensors. Using Weyl's tube formula, we turn this question into a differential geometric one involving the study of metric invariants of the real Veronese variety. More precisely, we give an explicit formula for its reach and curvature coefficients with respect to the Bombieri-Weyl metric. These results are obtained using techniques from Random Matrix theory and an explicit description of the second fundamental form of the Veronese variety in terms of GOE matrices. Our findings give a complete solution to the original problem, and in the case of rational normal curves lead to some novel asymptotic results.

Andrea Rosana
SISSA (Triest)
arosana@sissa.it

Antonio Lerario
SISSA (Trieste)
KTH (Stockholm)
lerario@sissa.it

Alberto Cazzaniga
AREA Science Park (Trieste)
alberto.cazzaniga@areasciencepark.it

MS59

Cancer Classification and Pathway Discovery Using Non-Negative Tensor Factorization

The tumor microenvironment (TME) refers to the intricate environment surrounding the tumor, where cancer cells interact with various components such as stromal, immune, vascular, and extracellular elements. Recently, there has been a growing acknowledgment of the TME's critical role in influencing tumor growth, disease advancement, and responsiveness to treatments. A comprehensive study in this area requires the integration of data from multiple sources, including various modes and samples. We have built a generalizable probabilistic non-negative tensor factorization technique that can be applied broadly to integrate and analyze multi-modal, multi-sample datasets. In addition to our tensor-based framework, we have incorporated an ad-hoc statistical pipeline that further enhances our ability to generate robust and biologically relevant clusters (or factors) that can be used in downstream analysis. The methodologies we have developed through this effort will contribute to our knowledge of the TME in several ways. These include understanding the cellular heterogeneity that exists within the TME, identifying the communication between cells, and elucidating the intrinsic pathways that drive tumor growth and immune evasion.

Neriman Tokcan, Daniel Chafamo, Vignesh Shanmugam
Broad Institute of MIT and Harvard
neriman.tokcan@umb.edu, dchafamo@broadinstitute.org,
vshanmug@broadinstitute.org

MS60

Transcendental Properties of Entropy-Constrained Sets

For information-theoretic quantities with an asymptotic operational characterization, the question arises whether an alternative single-shot characterization exists, possibly including an optimization over an ancilla system. When the expressions are algebraic and the ancilla is finite, this leads to semialgebraic level sets. In this work, we provide a criterion for disproving that a set is semialgebraic, based on an analytic continuation of the Gauss map. Applied to the von Neumann entropy, this shows that its level sets are nowhere semialgebraic in dimension d ¿ 2, ruling out algebraic single-shot characterizations with finite ancilla (e.g., via catalytic transformations). We show similar results for related quantities, including relative entropy, mutual information, and Rnyi entropies.

Vjosa Blakaj
Technische Universität München
blakaj@ma.tum.de

Michael M. Wolf, Chokri Manai
Technical University of Munich
m.wolf@tum.de, chokri.manai@tum.de

MS60

Mutually Unbiased Bases: Polynomial Optimization and Symmetry

Two orthonormal bases of $\mathbb{C}^d$ are called mutually unbiased if the squared modulus of the inner product of any two vectors in distinct bases is equal to $1/d$. A natural question is for which pairs (d, k) there exist k mutually unbiased bases in dimension d. The (well-known) upper bound $d+1$ is attained when d is a power of a prime. For all other dimensions it is an open problem whether the bound $d+1$ can be attained. Navascus, Pironio, and Acn showed how to reformulate the existence question in terms of the existence of a certain C^*-algebra. This naturally leads to a noncommutative polynomial optimization problem and an associated hierarchy of semidefinite programs. The problem has a symmetry coming from the wreath product of the symmetric groups S_d and S_k. We exploit this symmetry (analytically) to reduce the size of the semidefinite programs making them (numerically) tractable. A key step is a novel explicit decomposition into irreducible modules of the space $\mathbb{C}^{dk}$ under the action of the above wreath product. We present numerical results for small d, k and low levels of the hierarchy. In particular, we obtain sum-of-squares proofs for the (well-known) fact that there do not exist $d+2$ mutually unbiased bases in dimensions $d = 2, 3, 4, 5, 6, 7, 8$. This is based on joint work with Sven Polak.

Sander Gribling
IRIF Paris University
gribling@irif.fr

Sven C. Polak
CWI
s.c.polak@tilburguniversity.edu

MS60

Border Ranks of Locally Positive and Invariant Tensor Decompositions

The Schmidt rank of a bipartite state is robust for approximations, as for every state, there is an ε-ball of elements having the same or larger rank. It is known that this statement is false for multipartite tensors. In particular, tensors exhibit a gap between their tensor rank and their border rank. The same behavior also applies to tensor network decompositions, for example, tensor networks with a geometry containing a loop. In this talk, we show that gaps between rank and border rank also occur for positive and invariant tensor decompositions. We present examples of nonnegative tensors and multipartite positive semidefinite matrices with a gap for several notions of positive and invariant tensor (network) decompositions. Moreover, we show a correspondence between certain types of quantum correlation scenarios and constraints in positive ranks. This allows showing that certain sets of multipartite probability distributions generated from local measurements on a tensor network state are not closed. Hence, testing the membership of these quantum correlation scenarios is impossible in finite time.

Andreas Klinger, Tim Netzer, Gemma De les Coves
University of Innsbruck
andreas.klingler@uibk.ac.at, tim.netzer@uibk.ac.at, gemmadelescoves@gmail.com

MS60

An Operator-Algebraic Formulation of Self-Testing

Suppose we have a physical system consisting of two separate labs, each capable of making a number of different measurements. If the two labs are entangled, then the measurement outcomes can be correlated in surprising ways. In quantum mechanics, we model physical systems like this with a state vector and measurement operators. However, we do not directly see the state vector and measurement operators, only the resulting measurement statistics (which are referred to as a “correlation”). There are typically many different models achieving a given correlation. Hence it is a remarkable fact that some correlations have a unique quantum model. A correlation with this property is called a self-test. In this talk, I'll introduce the standard definition of self-testing, discuss its achievements as well as limitations, and propose an operator-algebraic formulation of self-testing in terms of states on C^*-algebras. This new formulation captures the standard one and extends naturally to the commuting operator framework. I'll also discuss some related problems in operator algebras. Based on arXiv:2301,11291, joint work with Connor Paddock, William Slofstra, and Yangchen Zhou.

Yuming Zhao
University of Waterloo
Canada
y658zhao@uwaterloo.ca

Connor Paddock, William Slofstra, Yangchen Zhou
University of Waterloo
cpaulpad@uwaterloo.ca, weslofst@uwaterloo.ca, yangchen.zhou@uwaterloo.ca

MS61

Cylindrical Algebraic Coverings to determine satisfiability of non-linear polynomial constraints

The talk considers methods for determining the satisfiability of non-linear polynomial constraints over the reals. The most widely applicable symbolic methods for this are all variants of cylindrical algebraic decomposition (CAD). We focus on one such variant - cylindrical algebraic coverings - introduced in 2021 (doi:10.1016/j.jlamp.2020.100633). This algorithm follows a model driven approach with unsatisfiable models generalised to CAD cells which overlap: driving future search away from conflicts until either a satisfying point is found or a complete covering is produced. It is the backbone of the cvc5 solver for non-linear real arithmetic (https://doi.org/10.1007/978-3-030-99524-9_24) which is currently the state-of-the-art for such problems (see e.g. SMT Competition 2022). In the talk we will first introduce the underlying ideas of the algorithm. Then, in line with the session theme, discuss what certification is currently available for CAD based methods, and what hope the covering method may offer for progress here.

Matthew England
Coventry University
ab9797@coventry.ac.uk

MS61

Algebraic Geometry and Optimization

A common problem in applications is fitting data to a model. This requires an objective function that acts as a notion of ”distance” to points in and outside your model. Our main examples of non-linear objective functions are the Euclidean distance and the log-likelihood functions, which we then restrict to semi-algebraic sets. When passing over to the setting of complex algebraic geometry, the number of critical points of these functions is predetermined, regardless of the input data. This brings us to the topic of the talk: what are these numbers and how can we compute them? Can we classify the statistical models where there is a unique complex critical point?

Lukas Gustafsson
KTH
Department of Mathematics
lukasgu@kth.se

MS61

Minimal Euclidean Distance Degree of Segre-Veronese Varieties

The Euclidean Distance degree $\mathrm{EDdeg}_Q(X)$ of an algebraic variety X in an inner product space $(\mathbb{R}^N, Q)$ counts the number of complex critical points of the distance function

$x \in X \mapsto Q(v-x, v-x)$ from a generic point $v \in \mathbb{R}^N$ to X. Since this invariant of X depends on Q, it is a natural problem to find or characterize inner products Q that correspond to the minimal possible $\mathrm{EDdeg}_Q(X)$. In my talk I will discuss this question for Segre-Veronese varieties, which consist of rank-1 (partially symmetric) tensors. I will show that with respect to the classical Frobenius product $F(A,B) = \sum_{i=1}^{n}\sum_{j=1}^{m} A_{ij}B_{ij}$, the variety X of $n \times m$ rank-1 matrices has smallest $\mathrm{EDdeg}_F(X) = \min(n,m)$, whereas $\mathrm{EDdeg}_Q(X)$ with respect to a sufficiently general inner product Q on $\mathbb{R}^N = \mathbb{R}^{n\times m}$ is much higher.

Khazhgali Kozhasov
Friedrich-Schiller-Universität Jena
k.kozhasov@tu-braunschweig.de

MS61

Extrapolating Towards Singular Solutions of Polynomial Homotopies

A polynomial homotopy h(x,t) = 0, is a family of polynomial systems in x, where t is one parameter. The homotopy defines solution paths x(t). We consider the problem of tracking paths moving to a singularity, which may be isolated or not, which may be at infinity or not. Recent work (presented at CASC 2022) demonstrated the effectiveness of Richardson extrapolation to accurately compute the value of the parameter t in the homotopy, corresponding to the nearest singular solution. Preliminary computations shows the promise of Aitken extrapolation to accurately compute the coordinates x of the singular solution.

Kylash Viswanathan
University of Illinois Chicago
kviswa5@uic.edu

Jan Verschelde
University of Illinois, Chicago, U.S.
janv@uic.edu

MS62

Decomposition of Zero-Dimensional Persistence Modules via Rooted Subsets

We study the decomposition of zero-dimensional persistence modules, viewed as functors valued in the category of vector spaces factorizing through sets. Instead of working directly at the level of vector spaces, we take a step back and first study the decomposition problem at the level of sets. This approach allows us to define the combinatorial notion of rooted subsets. In the case of a filtered metric space M, rooted subsets relate the clustering behavior of the points of M with the decomposition of the associated persistence module. In particular, we can identify intervals in such a decomposition quickly. In addition, rooted subsets can be understood as a generalization of the elder rule, and are also related to the notion of constant conqueror of Cai, Kim, Mmoli and Wang. As an application, we give a lower bound on the number of intervals that we can expect in the decomposition of zero-dimensional persistence modules of a density-Rips filtration in Euclidean space: in the limit, and under very general circumstances, we can expect that at least 25% of the indecomposable summands are interval modules.

ngel Javier Alonso
University of Technology, Graz, Austria
alonsohernandez@tugraz.at

MS62

Persistence Diagram Bundles: A Multidimensional Generalization of Vineyards

In persistent homology, we often study how the topology of a data set varies as a single ”scale parameter” varies. It is an active area of research to develop new methods for analyzing how the topology of a data set changes as multiple parameters vary. For example, if a point cloud evolves over time, then one might be interested in using time as a second parameter. When there are only two parameters (e.g., a scale parameter and time), one can compute a ”vineyard,” which encodes how persistent homology (PH) changes over time. However, vineyards cannot be used when there are more than two parameters. For example, in many time-evolving point clouds, there are additional system parameters controlling the coordinates of the points, and distinct topological features may arise for different system parameters. Generally, one cannot use multiparameter PH, either, because the filtered complexes constructed from the point clouds at different times and different system parameters do not form a multifiltration. In recent work, I generalized the concept of a vineyard to a ”persistence diagram (PD) bundle,” in which a set of filtered complexes is parameterized by an arbitrary topological space. In this talk, I'll discuss what a PD bundle is, talk about an algorithm for efficiently computing piecewise-linear PD bundles, and show that PD bundles can exhibit ”monodromy,” unlike vineyards. I'll also talk about a connection to cellular sheaves.

Abigail Hickok
Columbia University
aghickok@gmail.com

MS62

Composition Series of Arbitrary Cardinality in Modular Lattices

We discuss a generalization of a composition series from the perspective of lattice theory. In particular, we will focus on the lattice of subobjects of a persistence module. We will show that persistence modules over a particular type of small category have a generalized composition series. In particular, any pair of these composition series has the same multiset of subfactors. We will then give an explicit description of the sub factors. Time permitting, we will discuss an important limitation that is inherently assumed for many persistence modules. This is joint work with Eric J. Hanson.

Daisie Rock
Ghent University
Job.Rock@UGent.be

MS62

Optimal Transport Stability in Multiparameter Persistence and Applications to Geometric Data Analysis

One-parameter persistence barcodes provide a concise summary of the changing topology of geometric data filtered by a single real-valued function. When they are equipped with an optimal transport distance, one-parameter barcodes are stable to perturbations of the filtration, enabling their use in machine learning, statistics, and optimization frameworks based on multi-scale geometry. Adaptations of the barcode to multiparameter filtrations have recently been introduced using relative homological algebra. However, the question of whether these multiparameter barcodes can be interpreted as measures satisfying optimal transport stability has proven to difficult. In this talk, I will provide positive answers to this question and demonstrate the practical relevance of these results in doing machine learning with geometric data.

Luis Scoccola
Northeastern University
l.scoccola@northeastern.edu

MS63
Partial Elimination Spectral Sequence and Its Applications

In this talk we introduce Green's partial elimination theory together with a spectral sequence and its applications. The theory gives a detailed analysis of linear projections from one point. One of the applications is a construction of counterexamples to the Eisenbud-Goto regularity conjecture, and it is different from the Rees(-like) algebra one of McCullough and Peeva.

Junho Choe
Korean Institute for Advanced Study
junhochoe@kias.re.kr

MS63
Klyachko Filtrations and Regularity of Equivariant Reflexive Sheaves

In the decade of 1990s, Klyachko gave a characterization of equivariant vector bundles and reflexive sheaves on toric varieties, by means of a collection of flags of vector spaces. In this talk, we use this theory to introduce a family of lattice polytopes $\{\Omega_t\}$ encoding the multigraded structure of the global sections of a reflexive sheaf $\mathcal{E}$ on a complete smooth toric variety X. When X is projective of Picard rank 2, this description can be made more explicit. In particular, we can provide bounds for some invariants of $\mathcal{E}$, and we find a recursive formula for computing the Hilbert polynomial of $\mathcal{E}$. Finally, we use these tools to find an upper bound for the multigraded regularity index of $\mathcal{E}$.

Martí Salat-Moltó
Universitat de Barcelona
marti.salat@ub.edu

MS63
The v-number of a Graded Ideal

The v-number is an algebraic invariant of a graded ideal introduced by Cooper et al. whose study was originally motivated by problems in algebraic coding theory. Although they have been introduced quite recently, v-numbers have inspired results also in commutative algebra and combinatorics. In this talk, I will provide an overview of the state-of-the-art, with a specific focus on the relation between v-numbers, Castelnuovo-Mumford regularity, and regularity index. Additionally, new results on v-numbers of binomial edge ideals will be presented. These results highlight the interplay between v-numbers and graph domination theory which has numerous applications in network design and routing computation problems (this is a joint work with Delio Jaramillo-Velez).

Lisa Seccia
Max Planck Institute for Mathematics in the Science
seccia@mis.mpg.de

MS64
Tropical Nash Equilibria and Oriented Matroids

We study Nash equilibria of tropical signed bimatrix games. This generalizes the work of [Allamigeon, Gaubert & Meunier, SIAM J. Discret. Math., 2023] in which payoff matrices are tropically nonnegative. To this purpose, we consider Nash equilibria over oriented matroids, which encompass both classical and tropical games. If time allows, we will also present a few results in the zero-sum case. Joint work with S. Gaubert and F. Meunier.

Xavier Allamigeon
INRIA and CMAP, Ecole Polytechnique, CNRS
xavier.allamigeon@inria.fr

Stephane Gaubert
INRIA and CMAP, Ecole Polytechnique
stephane.gaubert@inria.fr

Frédéric Meunier
École des Ponts ParisTech
frederic.meunier@enpc.fr

MS64
Ambitropical Convexity, Injective Hulls and Mean-Payoff Games

We introduce ambitropical convex cones, generalizing max-plus and min-plus convex cones. Ambitropical convex cones are defined as lattices equipped with an additive action. We show that they admit several characterizations. They coincide with the fixed-point sets of Shapley operators (dynamic programming operators of zero-sum games), parametrizing optimal stationary policies in mean-payoff problems. They also coincide with hyperconvex sets with an additive action. They are the ranges of canonical retractions, obtained by composing retractions on max-plus and min-plus convex cones. Moreover, there is a well defined notion of ambitropical hull, which turns out to be isometric to Isbell's injective hull for sets with an additive action, leading to an explicit construction of this injective hull. We finally study finitely generated ambitropical convex cones. These cones arise when considering deterministic mean-payoff games with finite action spaces. We show that they admit decompositions in terms of alcoved polyhedra of A_n type.

Marianne Akian, Stephane Gaubert
INRIA and CMAP, Ecole Polytechnique
marianne.akian@inria.fr, stephane.gaubert@inria.fr

Sara Vannucci
Czech Technical University in Prague
vanucsar@fel.cvut.cz

MS64
The Geometry of Parameterized Shortest Paths

One of the most basic classes of algorithmic problems in combinatorial optimization is the computation of shortest paths. Tropical geometry is a natural language to analyze parameterized versions where some of the arc weights are unknown. I will introduce this point of view, with a link to polyhedral geometry. Moreover, I will present an algorithm that computes these parameterized shortest paths and apply it to real world data from traffic networks.

Michael Joswig
Technische Universität Berlin, Germany
joswig@math.tu-berlin.de

Benjamin Schröter
KTH Stockholm
schroete@math.uni-frankfurt.de

MS64

Tropical Gradient Descent

The identification of the space of phylogenetic trees and the tropical Grassmannian [Speyer and Sturmfels 2004] has inspired recent work formalising statistics on the tropical projective torus. The calculation of tropical statistics such as Fermat-Weber points or Wasserstein distances has given rise to tropical optimisation problems. Applying classical gradient descent to such problems can produce locally stable but non-optimal solutions, whereas these local solutions are no longer stable when we restrict ourselves to descent along tropical geodesics. In this talk we discuss the comparative stability of solutions under classical and tropical gradient descent.

Roan Talbut
Imperial College London
r.talbut21@imperial.ac.uk

Daniele Tramontano
Technical University of Munich
daniele.tramontano@tum.de

Mathias Drton
Technische Universität München, Germany
mathias.drton@tum.de

Anthea Monod, Yueqi Cao
Imperial College London
a.monod@imperial.ac.uk, y.cao21@imperial.ac.uk

MS65

Elimination Theory and Sparse Resultants in Algebraic Vision

In this talk, we will look at the sparse resultants in elimination theory and their applications to algebraic vision from a computational point-of-view. Specifically, the Sylvester-style matrices are usually preferred for resultant computation, on account of their simplicity. The system of equations arising in algebraic vision due to the camera geometry problems consist of Laurent polynomials with non-generic coefficients. The objective then is to generate softwares for estimating solutions to these systems in a robust manner, the so-called minimal solvers. Non-genericity, however, presents an algorithmic challenge in generating solvers, specifically if we restrict ourselves to using only the Sylvester-style matrices. Moreover, the usually desired determinantal form of the resultant is not always guaranteed. To this end, we will review two methods for generating sparse resultant-based minimal solvers for non-generic polynomial systems. One method uses the Sylvester-style matrix while the other method uses a variant of the u-resultant. The usefulness of both methods will be reviewed through experimental results in terms of solver speed and stability for selected problems in algebraic vision. We will also revisit the alternative multiplication matrix and grobner basis-based approach for generating minimal solvers, and discuss the connections between the two methods. We will conclude with certain open challenges in polynomial solving for algebraic vision.

Snehal Bhayani
University of Oulu
snehal.bhayani@oulu.fi

Zuzana Kukelova
Czech Technical University in Prague
kukelova@gmail.com

Janne Heikkilä
University of Oulu
janne.heikkila@oulu.fi

MS65

Learning to Solve Hard Minimal Problems

We present an approach to solving hard geometric optimization problems in the RANSAC framework. The hard minimal problems arise from relaxing the original geometric optimization problem into a minimal problem with many spurious solutions. Our approach avoids computing large numbers of spurious solutions. We design a learning strategy for selecting a starting problem-solution pair that can be numerically continued to the problem and the solution of interest. We demonstrate our approach by developing a RANSAC solver for the problem of computing the relative pose of three calibrated cameras, via a minimal relaxation using four points in each view. On average, we can solve a single problem in under 70 s. We also benchmark and study our engineering choices on the very familiar problem of computing the relative pose of two calibrated cameras, via the minimal case of five points in two views.

Petr Hruby
ETH Zurich
petr.hruby@inf.ethz.ch

Timothy Duff
University of Washington
Seattle, WA
timduff@uw.edu

Anton Leykin
School of Mathematics
Georgia Institute of Technology
leykin@math.gatech.edu

Tomas Pajdla
Czech Technical University in Prague
pajdla@cvut.cz

MS65

Algebra and Geometry of Camera Resectioning

In joint work with with Erin Connelly and Tim Duff, we study certain algebraic varieties associated with the camera resectioning problem. We characterize these resectioning varieties' multigraded vanishing ideals, and we derive and re-interpret celebrated results in computer vision due to Carlsson, Weinshall, and others related to camera-point duality. We also clarify some relationships between the classical problems of optimal resectioning and triangulation, state a conjectural formula for the Euclidean distance degree of a resectioning variety, and discuss how this conjecture relates to the recently-resolved multiview conjecture for triangulation varieties.

Jessie Loucks-Tavitas
University of Washington
jaloucks@uw.edu

MS65

Compatability of Fundamental Matrices for Complete Graphs

A set of fundamental matrices is said to be compatible if a set of cameras exists for which they are the fundamental matrices. We focus on the complete graph, where fundamental matrices for each pair of cameras are given. Previous work has established necessary and sufficient conditions for compatibility as rank and eigenvalue conditions on the n-view fundamental matrix obtained by concatenating the individual fundamental matrices. In this talk, we show that the eigenvalue condition is redundant. We provide explicit homogeneous polynomials that describe necessary and sufficient conditions for compatibility in terms of the fundamental matrices and their epipoles. In this direction, we find that quadruple-wise compatibility is enough to ensure global compatibility for any number of cameras. We demonstrate that for four cameras, compatibility is generically described by triple-wise conditions and one additional equation involving all fundamental matrices.

Felix Rydell
KTH
felixry@kth.se

Martin Bråtelund
University of Oslo
mabraate@math.uio.no

MS66

Fast Subgroup Membership Testing and Hashing on Pairing-Friendly Curves

Recently, Scott proposed efficient methods for subgroup membership testings for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ on the BLS family. In this talk, we generalize these methods and show that the new techniques are applicable to a large class of pairing-friendly curves. In addition, we also propose a general method for hashing to $\mathbb{G}_2$ on curves with the lack of twists. On this basis, we further optimize the general algorithm on curves with non-trivial automorphisms, which is suitable for BW13-P310 and BW19-P286.

Yu Dai
Sun Yat-sen University, China
daiy39@mail2.sysu.edu.cn

MS66

Pairings in Rank-1 Constraint Systems

Bilinear pairings have been used in different cryptographic applications and demonstrated to be a key building block for a plethora of constructions. In particular, some Succinct Non-interactive ARguments of Knowledge (SNARKs) have very short proofs and very fast verification thanks to a multi-pairing computation. This succinctness makes pairing-based SNARKs suitable for proof recursion, that is proofs verifying other proofs. In this scenario one requires to express efficiently a multi-pairing computation as a SNARK arithmetic circuit. Other compelling applications such as verifying BonehLynnShacham (BLS) signatures or KateZaveruchaGoldberg (KZG) polynomial commitment opening in a SNARK fall into the same requirement. The implementation of pairings is challenging but the literature has very detailed approaches on how to reach practical and optimized implementations in different contexts and for different target environments. In this talk we address the question of efficiently implementing a pairing as a SNARK arithmetic circuit. In this work, we consider Rank-1 Constraint Systems (R1CS), a widely used model to express SNARK statements. We implement our techniques in the gnark open-source ecosystem for BLS curves of embedding degree 12 and 24.

Youssef El Housni
Consensys
youssef.elhousni@consensys.net

MS66

Efficiently Computing a Pairing: Tricks Old and New

In an early text on Elliptic curves, Alfred Menezes observed that the computation of the Weil pairing took around 5 minutes on contemporary hardware. Of course then pairings were only of significance as a means of cryptanalysis of certain curves that failed the so-called MOV condition. Once pairings became tools for cryptography, it became apparent that significant speed-up was going to be required if pairing based cryptography were ever to become practical. Cryptographers rose to the challenge, and now a secure pairing can be calculated in well under a millisecond. This illustrates how, with sufficient effort, the impractical can become practical (those interested in Fully Homomorphic Encryption take note!) Here we review the journey, introduce some new ideas, plug some gaps, and highlight some less well known tricks.

Michael Scott
Technical Innovation Institute
Technical Innovation Institute
michael.scott@tii.ae

MS66

Accurately Benchmarking Efficiency of Pairing-Based Attribute-Based Encryption

Measuring efficiency is difficult, and therefore schemes might not compare in the way we think. In the last decades, several works have contributed in the quest to successfully determine and compare the efficiency of pairing-based attribute-based encryption (ABE) schemes. However, many of these works are limited: they use little to no optimizations, or use underlying pairing-friendly elliptic curves that do not provide sufficient security anymore. Hence, using these works to benchmark ABE schemes does not yield accurate results. In this talk, we present a framework for accurately benchmarking efficiency of ABE: ABE Squared, published at CHES 2022. In particular, we focus on uncovering the multiple layers of optimization that are relevant to the implementation of ABE schemes. Moreover, we focus on making any comparison fairer by considering the influence of the potential design goals on any optimizations. To this end, we also introduce manual, heuristic type-conversion techniques where existing techniques fall short. Finally, to illustrate the effectiveness of ABE Squared, we implement several schemes and provide all relevant benchmarks. These show that the design goal influences the optimization approaches, which in turn influence the overall efficiency of the implementations. Importantly, these demonstrate that the schemes also compare differently than existing works previously suggested.

Marloes Venema
Radboud University Nijmegen, The Netherlands
mvenemacrypto@gmail.com

MS67

Code-based Hash and Sign Primitives and Wave Signature Scheme

We present in this talk how to build hash and sign signature schemes whose security relies on code-based assumptions as the generic decoding problem. The construction is based on the use of trapdoor one-way functions that are Preimage Sampleable on Average (PSA). Then we will present an instantiation: the Wave-PSA family. The trapdoor function is one-way under two computational assumptions: the hardness of generic decoding for high weights and the indistinguishability of generalized $(U, U+V)$-codes. The preimage sampleable property (giving the proper distribution for the trapdoor inverse output) is ensured by including rejection sampling as we will show.

Thomas Debris-Alazard
INRIA Saclay
thomas.debris@inria.fr

MS67

Code-Based Signatures from Secure Multiparty Computation

Zero-knowledge proofs of knowledge are useful tools for designing signature schemes. Among the existing techniques, the MPC-in-Head (MPCitH) paradigm provides a generic framework to build quantum-resilient proofs using techniques from secure multiparty computation. This paradigm has recently been improved in a series of works which makes it an effective and versatile tool. In this talk, I will present the recent advances in code-based signatures relying on the MPC-in-the-Head framework. After a general introduction to MPCitH, I will describe the Syndrome-Decoding-in-the-Head signature scheme. The latter uses this paradigm to propose a new efficient signature scheme based on the syndrome decoding problem for random linear codes. This scheme outperforms all the former code-based schemes for the common "signature size + public key size" metric. Then, I will provide an overview of the follow-up works, which either optimize the paradigm or propose alternative constructions relying on it.

Thibauld Feneuil
Sorbonne University
thibauld.feneuil@cryptoexperts.com

MS67

Take Your Meds: Digital Signatures from Matrix Code Equivalence

Code equivalence is a relatively new approach to constructing post-quantum cryptography with interesting properties: it is easy to understand, flexible, and signatures are not too large. Specifically code equivalence in the rank metric seems suitable for signatures, and in this work we show how to build such a scheme by applying the Fiat Shamir transform to an identification scheme that is standard for equivalence/isomorphism problems. The resulting scheme is called MEDS, and we apply several tricks from the literature to achieve compact and secure signatures. The flexibility of code equivalence then furthermore shows us to easily adapt this scheme to create group and ring signature schemes. Driving further into matrix code equivalence, we show that it connects in several surprising ways to equivalence problems in multivariate cryptography and to the alternating trilinear forms equivalence. Furhtermore, matrix code equivalence generalized both Hamming code equivalence and sum rank code equivalence problems. All together, this places MCE at the heart of a general set of equivalence and isomorphism problems, and allows us to give a concrete security analysis for MEDS.

Krijn Reijnders
Radboud University
krijn@cs.ru.nl

MS67

Zero Knowledge Protocols and Signatures from the Restricted Syndrome Decoding Problem

The Restricted Syndrome Decoding Problem (R-SDP) corresponds to the Syndrome Decoding Problem (SDP) with the additional constraint that entries of the solution vector must live in a desired subset of a finite field. In this talk we describe how the problem can be used to obtain signature schemes with competitive performances. As major differences with the canonical SDP setting, we have a different notion of isometry and, taking into account state-of-the-art attacks, can use smaller codes. Also, the problem can be specialized (technically, requiring that the solution of R-SDP is an element of some subgroup with sufficiently large order), so that restricted objects (e.g., vectors) can be represented with a number of bits that is slightly larger than the security parameter. This enables the design of Zero Knowledge (ZK) protocols with very tight parameters. We demonstrate the effectiveness of these considerations by presenting a signature scheme that achieves signatures in the order of 7 kB, for 128 bits of security

Paolo Santini
Marche Polytechnic University
p.santini@staff.univpm.it

MS68

Minimal Codes and Strong Blocking Sets

A linear code is said to be minimal if the support of each of its codewords does not contain the support of any other independent codeword, namely, all its codewords are minimal. The study of minimal codewords arises from their applications to secret sharing schemes and to decoding strategies. They have recently been shown to correspond to strong blocking sets which are sets of projective points, such that their intersection with each hyperplane generates the hyperplane itself. In this talk we introduce the concepts of outer minimal codes and outer strong blocking sets. These are codes whose concatenation with minimal codes is minimal and sets whose field reduction is a strong blocking set. We investigate their structure and provide bounds on their length/size. We discuss an improvement on the best-known upper bound on the minimum size of a strong blocking set. Finally, we present a geometric construction of small strong blocking sets, with low computational cost. This is a joint work with Martino Borello and Alessandro Neri.

Gianira Alfarano

Eindhoven University of Technology
g.n.alfarano@tue.nl

Martino Borello
University of Paris 8
martino.borello@univ-paris8.fr

Alessandro Neri
Ghent University
alessandro.neri@ugent.be

MS68

Blocking Sets, Minimal Codes and Trifferent Codes

We prove new upper bounds on the smallest size of affine blocking sets, that is, sets of points in a finite affine space that intersect every affine subspace of a fixed codimension. We show an equivalence between affine blocking sets with respect to codimension-2 subspaces that are generated by taking a union of lines through the origin, and strong blocking sets in the corresponding projective space, which in turn are equivalent to minimal codes. Using this equivalence, we improve the current best upper bounds on the smallest size of a strong blocking set in finite projective spaces over fields of size at least 3. Furthermore, using coding theoretic techniques, we improve the current best lower bounds on strong blocking set. Over the finite field $\mathbb{F}_3$, we prove that minimal codes are equivalent to linear trifferent codes. Using this equivalence, we show that any linear trifferent code of length n has size at most $3^{n/4.55}$, improving the recent upper bound of Pohoata and Zakharov. Moreover, we show the existence of linear trifferent codes of length n and size at least $\frac{1}{3}\left(9/5\right)^{n/4}$, thus matching the best lower bound on trifferent codes. We also give explicit constructions of affine blocking sets with respect to codimension-2 subspaces that are a constant factor bigger than the best-known lower bound. By restricting to $\mathbb{F}_3$, we obtain trifferent codes of size at least $3^{n/48}$.

Anurag Bishnoi
Delft University of Technology
a.bishnoi@tudelft.nl

MS68

Saturating Systems and Covering Radius in the (sum-)rank Metric

The relationship between linear codes and sets of points in finite geometries have long been exploited by researchers, in fact it is a standard approach to construct generator matrices or parity check matrix of a linear code from a set of projective points. In this context, the supports of the codewords correspond to complements of hyperplanes in a fixed projective set, and this can be used to construct codes with bounded covering radius, related to saturating sets in projective space. The covering radius of a code is the least positive integer ρ such that the union of the spheres of radius ρ about each codeword equals the full ambient space. This fundamental coding theoretical parameter has been widely studied for codes in respect of the Hamming-metric. In this talk, we introduce the notion of saturating systems and their properties. In analogy with codes for the Hamming-metric, it turns out that a rank ρ-saturating system corresponds to a linear code of rank-metric covering radius ρ. Such codes have the property that every element of the ambient space is within rank-distance at most ρ of some codeword. Finally, we will also show how this approach can be also extended to the sum-rank metric.

Matteo Bonini
Aalborg University
mabo@math.aau.dk

Martino Borello
University of Paris 8
martino.borello@univ-paris8.fr

Eimear Byrne
UC Dublin
ebyrne@ucd.ie

MS68

Geometric Dual and Sum-Rank Minimal Codes

In this talk we will present some results about minimal codes in the sum-rank metric. These objects, introduced in [4], form a bridge between the classical minimal codes in the Hamming metric, the subject of intense research over the past three decades partly because of their cryptographic properties [2], and the more recent rank-metric minimal codes [1]. They have rich connections with geometry, as shown in [1,3,4] and references therein. We will illustrate these connections, together with some bounds on their parameters and some existence results. Via a tool that we name geometric dual, we manage to construct minimal codes with few weights. A generalization of the celebrated Ashikhmin-Barg condition is proved and used to ensure minimality of certain constructions. This is a joint work with Ferdinando Zullo. [1] G. N. Alfarano, M. Borello, A. Neri, and A. Ravagnani. *Linear cutting blocking sets and minimal codes in the rank metric.* Journal of Combinatorial Theory, Series A, 192:105658, 2022. [2] J. L. Massey. *Minimal codewords and secret sharing.* In Proceedings of the 6th joint Swedish-Russian international workshop on information theory, pages 276279, 1993. [3] A. Neri, P. Santonastaso, and F. Zullo. *The geometry of one-weight codes in the sum-rank metric.* Journal of Combinatorial Theory, Series A, 194:105703, 2023. [4] P. Santonastaso and F. Zullo. *On subspace designs.* arXiv:2204.13069, 2022.

Martino Borello
University of Paris 8
martino.borello@univ-paris8.fr

MS69

Operations Preserving Spectrahedrality

A major open question in the theory of hyperbolic polynomials is whether every hyperbolicity cone is a spectrahedron, meaning that it can be described by a linear matrix inequality. In this talk, we study when certain operations preserving hyperbolicity or stability also preserve the corresponding hyperbolicity cones to be spectrahedral.

Mario Kummer
Technische Universität Dresden
mario.kummer@tu-dresden.de

MS69

Symmetrically Hyperbolic Polynomials

We will be discussing symmetric polynomials (polynomials invariant under permutations of their variables) which are hyperbolic with respect to the all-one's vector. We will show that there is a correspondence between these polynomials and certain transformations of univariate polynomials preserving hyperbolicity. Within a class of symmetric polynomials, we characterize the hyperbolic ones using the Brnden-Borcea characterization of linear hyperbolicity preservers. Along the way, we will give related results concerning linear maps that only preserve hyperbolicity on a subspace of the univariate polynomials. We also give some connections to symmetric sums of squares and a number of conjectures about extensions of these results, which are supported by computer analysis.

Kevin Shu
Georgia Institute of Technology
kshu8@gatech.edu

MS69

Interlacing Properties for Combinatorial Generating Polynomial in Discrete Geometry

Generalizations of real-rooted polynomials to multivariate stable polynomials, and more recently lorentzian polynomials, have been used in a variety of settings to deduce distributional properties of combinatorial generating polynomials such as unimodality, log-concavity and gamma-positivity. Of recent interest in enumerative combinatorics is a stronger condition than unimodality known as the alternatingly increasing property. Recent work has shown that the real-zeros of polynomials can be used to deduce when the alternatingly increasing property holds as well, while additionally implying stronger properties such as bi-gamma-positivity. We will discuss some of the recent methodology developed for deducing such properties by way of the real zeros of polynomials, present their applications to examples including families of permutation statistics and Ehrhart h^*-polynommials, and point out some resulting questions of potential interest.

Liam Solus
KTH Royal Institute of Technology
solus@kth.se

MS70

Moment Problem for Algebras Generated by a Nuclear Space

In this talk we consider when a linear functionals defined on a unital commutative real algebra A, which we assume to be generated by a vector space V endowed with a Hilbertian seminorm q can be represented by a Radon measure. We characterize the functionals which can be represented by measures supported on the characters of A whose restrictions to V are $q-$continuous. We apply this characterization to V endowed with a nuclear topology to derive new and to provide alternative proofs of already known results. These results are the analogues for the power moment of the Bochner-Minlos theorem for the trigonometric moment problem or the inverse problem for the Fourier-Laplace transform. This talk is based on a joint paper with Maria Infusino, Salma Kuhlmann, Patrick Michalski, for more details see https://arxiv.org/abs/2301.12949

Tobias Kuna
Università degli Studi dell'Aquila
tobias.kuna@univaq.it

Salma Kuhlmann
University of Konstanz, Germany
salma.kuhlmann@uni-konstanz.de

Maria Infusino
University of Cagliari, Italy
maria.infusino@unica.it

Patrick Michalski
NA
patrick.michalski@googlemail.com

MS70

Real and Complex Geometry of Polygons and their Adjoint Curves - Part I

Given a convex polygon in the real plane with d vertices, its adjoint is the unique curve of degree $d-3$ passing through the intersection points of the boundary lines lying off the boundary of the polygon. This is a special case of a construction due to Wachspress (1975). We study the real and complex geometry of the map taking a polygon to its adjoint. Of particular interest is the case $d = 7$ for which the map is dominant and finite of degree of 864.

Daniele Agostini
Eberhard Karls Universität Tübingen
daniele.agostini@uni-tuebingen.de

Daniel Plaumann
TU Dortmund
daniel.plaumann@math.tu-dortmund.de

Rainer Sinn
University of Leipzig
rainer.sinn@uni-leipzig.de

Jannik L. Wesner
TU Dortmund University
jannik.wesner@tu-dortmund.de

MS70

Real and Complex Geometry of Polygons and their Adjoint Curves - Part II

Given a convex polygon in the plane with d vertices, its adjoint is the unique curve of degree $d-3$ passing through the intersection points of the boundary lines lying off the boundary of the polygon. This is a special case of a construction due to Wachspress (1975). This second part focuses on a geometric construction for $d = 6$ and the intricate real geometry for $d = 7$.

Jannik L. Wesner
TU Dortmund University
jannik.wesner@tu-dortmund.de

MS70

Error Bounds And Singularity Degree In Semidefinite Programming

In semidefinite programming a proposed optimal solution may be quite poor in spite of having sufficiently small residual in the optimality conditions. This issue may be framed in terms of the discrepancy between forward error (the unmeasurable "true error") and backward error (the measurable violation of optimality conditions). In [SIAM J. Optim., 10 (2000), pp. 1228–1248], Sturm provided an upper bound on forward error in terms of backward error and singularity degree. In this work we provide a method to bound the maximum rank over all optimal solutions and use this result to obtain a lower bound on forward error for a class of convergent sequences. This lower bound complements the upper bound of Sturm. The results of Sturm imply that semidefinite programs with slow convergence necessarily have large singularity degree. Here we show that large singularity degree is, in some sense, also a sufficient condition for slow convergence for a family of external-type "central" paths. Our results are supported by numerical observations.

Hugo Woerdeman
Drexel University
hugo@math.drexel.edu

Stefan Sremac
Pacific Union College
ssremac@puc.edu

Henry Wolkowicz
University of Waterloo
hwolkowicz@uwaterloo.ca

MS71

New Methods for Phylogenetic Reconstruction Based on Algebraic Tools

The main goal of phylogenetics is the inference of the evolutionary relationships between species or other biological entities. These relationships are usually represented as a tree graph, where leaves represent the current species and the interior nodes correspond to the (possibly extincted) ancestors. In this setting, phylogenetic reconstruction methods attempt to infer the shape of these tree graphs from the information available in an arrangement of the DNA sequences of the species. In this talk we will present a pair of new reconstruction methods, SAQ and ASAQ, which take advantage of the algebraic and semi algebraic information available in the data to reconstruct the phylogenetic tree. We will explain briefly the mathematical basis of both methods and will show their performance on simulated and real data.

Jesus Fernandez Sanchez
Universitat Politechnica de Catalunya
jesus.fernandez.sanchez@upc.edu

Marta Casanellas
Departament de Matematiques
Universitat Politècnica de Catalunya
marta.casanellas@upc.edu

Marina Garrote López
University of British Columbia
mgarrote@math.ubc.ca

MS71

Moments of Step Functions and Allele Frequency Spectra

In this talk, we present work on the univariate moment problem of piecewise-constant density functions on the interval $[0, 1]$ and its consequences for an inference problem in population genetics. We show that, up to closure, any collection of n moments is achieved by a step function with at most $n-1$ breakpoints and that this bound is tight. We use this to show that any point in the nth coalescence manifold in population genetics can be attained by a piecewise constant population history with at most $n-2$ changes. Both the moment cones and the coalescence manifold are projected spectrahedra and we describe the problem of finding a nearest point on them as a semidefinite program.

Georgy Scholten
Sorbonne Université
georgy.scholten@lip6.fr

Zvi Rosen
Florida Atlantic University
rosenz@fau.edu

Cynthia Vinzant
North Carolina State University
U.S.
vinzant@uw.edu

MS71

Wasserstein Distances on Tropical Projective Torii of Different Dimensions

Phylogenetic Trees are a fundamental tool for summarising the mutation structure of many diseases. In practice, we cannot identify the exact tree, but instead identify a posterior distribution on the space of all trees with the observed leaf set. Wasserstein distances are a popular tool for comparing distributions, but require our measures to live in the same space; this is generally not the case when studying the phylogenetic trees of independent evolutionary processes. To this end, we define Wasserstein distances between measures on tree spaces of different dimensions. Using the tropical interpretation of tree space [Speyer and Sturmfels, The Tropical Grassmannian], we study optimal transport between general measures on tropical projective torii. Our method mirrors the semi-orthogonal map methodology used by Cai and Lim [Cai and Lim, Distances Between Probability Distributions of Different Dimensions] in the Euclidean setting, establishing the same powerful behaviour in a more complex tropical setting. We also establish an algorithm for computing this tropical Wasserstein distance across different dimensions in practice.

Roan Talbut
Imperial College London
r.talbut21@imperial.ac.uk

Daniele Tramontano
Technical University of Munich
daniele.tramontano@tum.de

Mathias Drton
Technische Universität München, Germany
mathias.drton@tum.de

Anthea Monod
Imperial College London
a.monod@imperial.ac.uk

MS72

Degrees of No-Three-Way Interaction Models

In this talk I will discuss a formula for the degrees and maximum likelihood degrees of no-three-way interaction models involving at least one binary variable. This extends formulae by Amendola et al. and Coons et al. I will discuss how these numbers naturally arise as the evaluation of the Tutte polynomial of the complete bipartite graph, and to what extent these results can be generalized. This is joint work with Aida Maraj.

Taylor Brysiewic
Western University
tbrysiew@uwo.ca

Aida Maraj
University of Michigan
maraja@umich.edu

Aida Maraj
Max Planck Institute for Mathematics in the Sciences
maraja@umich.edu

MS72

A Discovery Algorithm for Cyclic Causal Graphs under Non-Gaussian Linear Models

During this talk, we will explore the problem of identifying the underlying structure of cyclic linear non-Gaussian causal models. Our focus is on recovering the combinatorial graph structure of random variables within a linear structural equation model that includes non-Gaussian error terms. We characterize when certain determinants of sub-tensors of the higher-order moment tensors vanish and develop reliable test statistics based on these algebraic relationships. Our proposed algorithm utilizes these higher-order moment tensors to iteratively identify the cycles of the graph and the causal relationships between them.

Marina Garrote López
University of British Columbia
mgarrote@math.ubc.ca

Mathias Drton
Technische Universität München, Germany
mathias.drton@tum.de

Niko Nikov, Elina Robeva
University of British Columbia
niko.a.nikov@gmail.com, erobeva@math.ubc.ca

MS72

Toward Standard Imsets of Maximal Ancestral Graphs

The imsets of [Studney, Probabilistic conditional independence structures, etc] are an algebraic method for representing conditional independence models. They have many attractive properties when applied to such models, and they are particularly nice for working with directed acyclic graph (DAG) models. In particular, the 'standard' imset for a DAG is in one-to-one correspondence with the independences it induces, and hence is a label for its Markov equivalence class. We present a proposed extension to standard imsets for maximal ancestral graph (MAG) models, using the parameterizing set representation of [Hu, Faster algorithms for Markov equivalence, etc]. By construction, our imset also represents the Markov equivalence class of the MAG. We show that for many such graphs our proposed imset is *perfectly Markovian* with respect to the graph thus providing a scoring criteria by measuring the discrepancy for a list of independences that define the model; this gives an alternative to the usual BIC score that is much easier to compute. We prove that it does work for *simple* MAGs, where all heads have size less than three, as well as for a large class of purely bidirected models. We also show that, of independence models that do represent the MAG, the one we give is the simplest possible. Further we refine the ordered local Markov property, which relates to finding the best imsets representing general MAGs.

Zhongyi Hu
University of Oxford
Department of Statistics
zhongyi.hu@keble.ox.ac.uk

MS72

Colored Gaussian Graphical Models with Toric Vanishing Ideals

A Colored Gaussian graphical model is a collection of multivariate Gaussian distributions in which a colored graph encodes conditional independence relations among the random variables. Its set of concentration matrices is a linear space of symmetric matrices intersected with the cone of positive definite matrices. Its inverse space, the space of covariance matrices, on the contrary, most often is not a friendly variety. We are interested in the equations that vanish on the covariance matrices of these models. The main result of the talk is that colored Gaussian graphical models with block graph structure that satisfy certain permutation symmetries (RCOP) are toric in the space of covariance matrices. We provide explicit Markov bases/generating sets for the vanishing ideal of this variety which can be read from paths in the graph.

Jane Coons
St John's College, University of Oxford
jane.coons@sjc.ox.ac.uk

Aida Maraj
Max Planck Institute for Mathematics in the Sciences
maraja@umich.edu

Aida Maraj
University of Michigan
maraja@umich.edu

Pratik Misra
KTH Royal Institute of Technology
pratikm@kth.se

Miruna-Stefana Sorea
SISSA, Trieste and RCMA ULBS
SISSA, Trieste and RCMA ULBS
miruna.stefana.sorea2019@gmail.com

MS73

Unique Powers-of-forms Decompositions From Simple Gram Spectrahedra

In powers-of-forms (POF) decomposition, we are given forms f_d of degree $d \cdot k$ in n variables for (various) values $d \in D$, e.g. $D = \{0, 1, 2, 3\}$, and we are asked to find k-forms $q_1, \ldots, q_m$ such that $f_d = \sum_{i=1}^{m} q_i^d$ for all $d \in D$. For fixed d, this amounts to finding a k-Waring decomposition of f of rank m. It turns out that if $d \geq 3$ and m is not too large, general POF decompositions of rank m will be unique for the forms they describe, up to trivialities. The algorithmic task to recover the unique addends of a POF decomposition is poorly understood, but has applications in algebraic statistics, as e.g. the parameter estimation problem for mixtures of centered Gaussians from moments is a POF problem, where $k = 2$. We aim to understand for which ranks m, recovering the unique addends of some typical rank-m POF decomposition is possible with an efficient algorithm. In this talk, I generalize a classical algorithmic uniqueness result for 1-Waring decompositions to the case of all $k \geq 1$. The key ingredient is a condition that the second order power sum $\sum_{i=1}^{m} q_i^2$ has a particularly simple Gram spectrahedron.

Alexander Blomenhofer
CWI Amsterdam, Netherlands
alexander.blomenhofer@cwi.nl

MS73
Reach of the Segre Variety

We compute the reach and the the second fundamental form of the (spherical) real Segre-Veronese variety; i.e., the manifold of rank-one partially symmetric tensors in $\mathbb{R}^{n_1\times\cdots\times n_d}$ of norm one. In particular, we show that the reach only depends on the dimension d of the tensor, but not on the size of its modes $n_1, \ldots, n_d$. This is joint work with Paul Breiding.

Sarah Eggleston
University of Osnabrück, Germany
seggleston@uni-osnabrueck.de

Paul Breiding
University Osnabrück
Germany
pbreiding@uni-osnabrueck.de

MS73
Tensors and Equilibria in Game Theory

In game theory, n tensors with the same format are used to describe an n-player game. Studying the equilibria of such games is analogous to identifying certain points in the same tensor space. I discuss certain situations where concepts such as Nash and correlated equilibria fall short of predicting the most beneficial outcome for all players and how this could be overcome via dependency equilibrium. This talk will feature connections to real algebraic varieties, oriented matroids, and algebraic statistics.

Irem Portakal
Otto-Von-Guericke Universität Magdeburg
irem.portakal@tum.de

Bernd Sturmfels
MPI Leipzig and UC Berkeley
bernd@mis.mpg.de

Javier Sendra-Arranz
MPI Leipzig
javier.sendra@mis.mpg.de

MS73
Higher-Order Moment and Cumulant Tensors in Factor Analysis Model

The factor analysis model is a statistical model where a certain number of hidden random variables, called factors, affect linearly the behavior of another set of observed random variables with additional random noise. The model's main assumption is that the factors and the noise are Gaussian random variables. This implies that the feasible set lies in the cone of positive semidefinite matrices. This work does not assume that the factors and the noise are Gaussian. Hence, the observed variables' higher-order moment and cumulant tensors are generally nonzero. This motivates the notion of kth-order factor analysis model, which is the family of all random vectors in a factor analysis model where the factors and the noise have finite and possibly nonzero moment and cumulant tensors up to order k. This subset may be described as the image of a polynomial map onto a Cartesian product of symmetric tensor spaces. In our work, we compute its dimension and provide conditions under which the image has positive codimension. This is joint work with Muhammad Ardiyansyah.

Luca Sodomaco, Muhammad Ardiyansyah
Aalto University
sodomaco@kth.se, muhammad.ardiyansyah@aalto.fi

MS74
Thermalization of Quantum Memories Using Tensor Networks

The aim of a quantum memory is to protect an encoded quantum state against errors for long periods of time. Heuristic arguments have long pointed to a weakness of 2D memories against thermal noise processes. In this talk I will present a rigorous estimate on the lifetime of a class of 2D memories under a noise process modelled by Davies generators which confirms this heuristic belief, i.e., that these memories are fragile at any finite temperature. The result is obtained by proving that the spectral gap of the generator is lower bounded by a positive constant uniformly in the system size. To obtain the lower bound on the spectral gap, I will show how to represent the invariant state of the thermal process as a Tensor Network state (in particular, a PEPS). This will allow us to use tools and techniques from tensor networks, in particular the ones used to show the spectral gap of the so-called Parent Hamiltonian, to estimate the gap of the generator of the thermal process.

Angelo Lucia
Universidad Complutense de Madrid
anglucia@ucm.es

MS74
Matrix Product Operator Algebras

Topological order in two dimensional systems is closely related to fusion categories. For example, in PEPS topological order emerges due to certain MPO symmetries of the defining tensors, where the MPOs themselves are identified with the fusion category. In this talk we show that the MPO symmetries can naturally be interpreted as representations of certain algebras (weak Hopf algebras), providing an alternative (but completely equivalent) language to talk about the MPO symmetries.

Andras Molnar
University of Vienna
Vienna, Austria
andras.molnar@univie.ac.at

MS74
The Minimal Canonical Form of a Tensor Network

Tensor networks have a gauge degree of freedom on the virtual degrees of freedom that are contracted. A canonical form is a choice of fixing this degree of freedom. For matrix product states, choosing a canonical form is a powerful tool, both for theoretical and numerical purposes. On the other hand, for tensor networks in dimension two or greater there is only limited understanding of the gauge symmetry. Here we introduce a new canonical form, the minimal canonical form, which applies to projected entangled pair states (PEPS) in any dimension, and prove a corresponding fundamental theorem. Already for matrix product states this gives a new canonical form, while in higher dimensions it is the first rigorous definition of a canonical form valid for any choice of tensor. We show that two tensors have the same minimal canonical forms if and only if they are gauge equivalent up to taking limits; moreover, this is the case if and only if they give the same quantum state for any geometry. In particular, this implies that the latter problem is decidable - in contrast to the well-known undecidability for PEPS on grids. We also provide rigorous algorithms for computing minimal canonical forms. To achieve this we draw on geometric invariant theory and recent progress in theoretical computer science in non-commutative group optimization. Joint work with Arturo Acuaviva, Visu Makam, Harold Nieuwboer, David Prez-Garca, Friedrich Sittner, and Freek Witteveen.

Harold Nieuwboer
University of Amsterdam
h.a.nieuwboer@uva.nl

Michael Walter
Ruhr Universitat Bochum
Germany
michael.walter@rub.de

MS74

Near Optimal Sample Complexity for Matrix and Tensor Normal Models via Geodesic Convexity

The matrix normal model, the family of Gaussian matrix-variate distributions whose covariance matrix is the Kronecker product of two lower dimensional factors, is frequently used to model matrix-variate data. The tensor normal model generalizes this family to Kronecker products of three or more factors. We study the estimation of the Kronecker factors of the covariance matrix in the matrix and tensor models. We show nonasymptotic bounds for the error achieved by the maximum likelihood estimator (MLE) in several natural metrics. In contrast to existing bounds, our results do not rely on the factors being well-conditioned or sparse. For the matrix normal model, all our bounds are minimax optimal up to logarithmic factors, and for the tensor normal model our bound for the largest factor and overall covariance matrix are minimax optimal up to constant factors provided there are enough samples for any estimator to obtain constant Frobenius error. In the same regimes as our sample complexity bounds, we show that an iterative procedure to compute the MLE known as the flip-flop algorithm converges linearly with high probability. Our main tool is geodesic strong convexity in the geometry on positive-definite matrices induced by the Fisher information metric. This strong convexity is determined by the expansion of certain random quantum channels.

Akshay Ramachandran
Centrum Wiskunde & Informatica (CWI)
Netherlands
akshay.ramachandran@cwi.nl

MS75

Application of Adaptive Annealing (AdaAnn) to Approximate Multimodal Posterior Distribution for Parameter Estimation

Normalizing flows are invertible mappings used to transform simpler probability densities into ones that are more complex. Through optimizing parameters associated with these mappings, normalizing flows are used in statistics and machine learning for density estimation and variational inference. In the framework of variational inference, to improve the efficiency and accuracy of the approximation via normalizing flows especially when a target distribution is multimodal, annealing of the target distribution in the optimization is often employed. This essentially creates a homotopy between the most annealed distribution and the wanted target distribution. A constant annealing schedule often applies slowly-changing temperatures to the target distribution and can be inefficient computationally. This talk will introduce a more efficient adaptive annealing schedule that automatically adjusts the incremental step in the annealing schedule to the KL-divergence between two adjacent tempered distributions called AdaAnn. We will demonstrate the computational efficiency of normalizing flows with AdaAnn in approximating multimodal distributions and obtaining Bayesian inferences of the parameters for a dynamical system with local identifiability degree larger than one.

Emma Cobian
University of Notre Dame
ecobian@nd.edu

Jonathan Hauenstein
University of Notre Dame
Dept. of App. Comp. Math. & Stats.
hauenstein@nd.edu

Fang Liu, Daniele E. Schiavazzi
University of Notre Dame
fang.liu.131@nd.edu, dschiavazzi@nd.edu

MS75

When Does Subtracting a Rank-one Approximation Decrease Tensor Rank?

Subtracting a critical rank-one approximation from a matrix always results in a matrix with a lower rank. This is not true for tensors in general. We ask the question: what is the closure of the set of those tensors for which subtracting a rank-one approximation does result in lowering the rank? In this talk, we show how to construct this variety of tensors and we show how this is connected to the bottleneck points of the variety of rank-one tensors and in general to the singular locus of the hyperdeterminant and to orthogonally decomposable tensors.

Emil Horobet
Department of Mathematics and Computer Science
Sapientia Hungarian University of Transilvania
horobetemil@ms.sapientia.ro

MS76

Computing Geometric Feature Sizes for Algebraic Manifolds

In computational topology and geometry, theoretical guarantees for algorithms often take the following form: Start with a finite sample of points from a subspace of $\mathbb{R}^n$. If the sample is ”dense enough” with respect to the subspace, then the algorithm outputs a quantity of interest for the subspace, for example its Betti numbers. The quantities associated to a subspace which determine how dense of a sample is necessary are well studied by computational geometers: the reach, local feature size, and weak feature size of a subspace. In this talk, I will discuss some new results and numerical algebraic geometry methods for computing the reach, weak feature size, and bottlenecks of algebraic manifolds. For instance, we are able to show that the real part of generic non-quadratic complete intersections have finitely many k-bottlenecks. This is an application of the Alexander-Hirschowitz theorem and is new for $k > 2$. I will also present some motivating computational results which combine our feature size computations with persistent homology and computational geometry methods.

Sandra Di Rocco
Department of Mathematics
KTH
dirocco@math.kth.se

Parker Edwards
University of Notre Dame
parker.edwards@nd.edu

David Eklund
Colorado State University
daek@kth.se

Oliver Gäfvert
KTH Stockholm
olivergafvert@gmail.com

Jonathan Hauenstein
University of Notre Dame
Dept. of App. Comp. Math. & Stats.
hauenstein@nd.edu

MS76

Conormal Spaces and Whitney Statifications

In this talk I will describe a new algorithm for computing Whitney stratifications of both real and complex algebraic varieties. The main ingredients are (a) an algebraic criterion, due to L and Teissier, which reformulates Whitney regularity in terms of conormal spaces and maps, and (b) a new interpretation of this criterion which can be practically implemented on a computer. This algorithm improves upon the existing state of the art by several orders of magnitude, even for relatively small input varieties. This algorithm gives rise to related algorithms for efficiently stratifying flags on a given variety, and algebraic maps. This is joint work with Vidit Nanda (Oxford).

Martin Helmer
North Carolina State University
mhelmer@ncsu.edu

Vidit Nanda
University of Oxford
nanda@maths.ox.ac.uk

MS76

Efficient Computation of a Semi-Algebraic Basis of the First Homology Group of a Semi-Algebraic Set

We give an algorithm for computing a semi-algebraic basis for the first homology group, $H_1(S, \mathbb{F})$, with coefficients in a field $\mathbb{F}$, of any given semi-algebraic set $S \subset R^k$ defined by a closed formula, where R is a real closed field. The complexity of the algorithm is bounded singly exponentially, that is, if the given quantifier-free formula involves s polynomials whose degrees are bounded by d, the complexity of the algorithm is bounded by $(sd)^{k^{O(1)}}$. This algorithm generalizes well known algorithms having singly exponential complexity for computing a semi-algebraic basis of the zero-th homology group of a semi-algebraic set, which is equivalent to the problem of computing a set of points meeting every semi-algebraically connected component of the given semi-algebraic set at a unique point.

Saugata Basu
Department of Mathematics, Purdue University
sbasu@purdue.edu

Sarah Percival
Michigan State University
perciva9@msu.edu

MS77

Principal Landau Determinants

The study of the singularities of Feynman integrals is a classical problem in scattering amplitudes. In perturbation theory, the Landau discriminant describes the leading singularities of the associated Feynman integral, by characterising when the Landau equations admit solutions. In this joint work with Sabastian Mizera and Simon Telen, we elaborate on the recent reformulation of Landau singularities of Feynman integrals allowing for practical applications in modern particle physics computations. The singularity locus is made rigorous by the principal Landau determinant, which is an object inspired by the work of Gelfand, Kapranov, and Zelevinsky (GKZ). It involves solving critical point equations for every facet of a certain Newton polytope. The UV/IR singularities appear as dominant components in the kinematic space and consistently stripped away. After highlighting differences between generic GKZ systems and Feynman integrals, we compute the principal Landau determinants for the infinite families of one-loop and banana diagrams with different mass configurations. We introduce a numerical sampling code that makes possible applications to more complicated diagrams.

Claudia Fevola
Max Planck Institute for Mathematics in the Sciences
claudia.fevola@mis.mpg.de

Simon Telen
MPI Leipzig
simon.telen@mis.mpg.de

Sebastian Mizera
Institute of Advanced Studies
smizera@ias.edu

MS77

Invitation to Positive Geometry

In recent years, combinatorics, algebra and geometry have become connected to particle physics and cosmology in novel and unexpected ways. Progress on scattering amplitudes and Feynman integrals has led to fascinating mathematical structures, such as the amplituhedron. The emerging field of Positive Geometry aims to unify and further develop these threads. This lecture offers a first glimpse and if offers an invitation to applied algebraic geometers to join the discussion.

Bernd Sturmfels
MPI Leipzig and UC Berkeley
bernd@mis.mpg.de

MS77

Computing Positroid Cells, Their Boundary and Dimension

Scattering amplitudes for the $N = 4$ SYM theory can be studied via the amplituhedron, a geometric object defined by Arkani-Hamed and Trnka as the image of the positive Grassmannian under a linear map. The geometry of the positive Grassmannian is encoded by positroids, a family of matroids introduced by Postnikov with a remarkable combinatorial structure. The images of these positroid cells are good candidates to decompose the amplituhedron. For this reason, it is interesting to study the dimension of the positroid cells and how they intersect. In this talk I will provide a new combinatorial characterization of positroids for $\mathrm{Gr}_{\geq 0}(2, n)$, the Grassmannians of lines and then discuss the generalization to higher Grassmannians. This characterization, in terms of graphs, can be used to easily compute the dimension, the intersection and the boundary of positroid cells. This relies on determining different ways to enlarge a given collection of subsets of $\{1, \ldots, n\}$ to represent the dependent sets of a positroid. This talk is based on [Mohammadi – Zaffalon, Computing positroid cells in the Grassmannian of lines, their boundaries and their intersections].

Francesca Zaffalon
KU Leuven
francesca.zaffalon@kuleuven.be

MS78

Topological Bounds for Tropical Varieties

During this talk, we will present several bounds for Betti numbers of tropical varieties, or more generally, for real algebraic varieties which can be constructed from the combinatorial patchworking process. We will mainly consider the hypersurface case and the zero dimensional case.

Frédéric Bihan
Université Savoie Mont Blanc
France
frederic.bihan@univ-smb.fr

MS78

Geometry Over the Tropical Hyperfield

The tropical hyperfield was introduced by Viro in his formulation of tropical geometry. On the other hand, the marriage of tropical geometry with F1-geometry brought forth a theory of tropical schemes. We merge these two perspectives into a joint formalism, which allows for a unifying theory for classical algebraic geometry and tropical geometry.

Oliver Lorscheid
IMPA
Brazil
oliver@impa.br

MS78

Tropical Ideals: Some Computational Aspects

Tropical ideals are ideals in the tropical polynomial semiring in which any bounded-degree piece is 'matroidal'. They were introduced as a sensible class of objects for developing algebraic foundations in tropical geometry. In this talk I will give some background on the theory of tropical ideals, present a few of the latest developments, and discuss a couple of open questions regarding their computational aspects.

Felipe Rincon
Queen Mary University of London
f.rincon@qmul.ac.uk

MS78

Monomial Ideals From Tropical Hyperplane Arrangements

We consider arrangements of tropical hyperplanes where the apices of the hyperplanes are taken to infinity in certain directions. Such an arrangement defines a decomposition of Euclidean space where a cell is determined by its 'type' data, analogous to the covectors of an oriented matroid. By work of Develin-Sturmfels and Fink-Rincn, these 'tropical complexes' are dual to subdivisions of root polytopes, which in turn are in bijection with mixed subdivisions of certain generalized permutohedra. Extending previous work with Joswig-Sanyal, we show how a natural monomial labeling of these complexes describes polynomial relations (syzygies) among 'type ideals' which arise naturally from the combinatorial data of the arrangement. This leads to novel ways of studying algebraic properties of various monomial and toric ideals, as well as relating them to combinatorial and geometric properties. In particular, our methods of studying the dimension of the tropical complex leads to new formulas for homological invariants of toric edge ideals of bipartite graphs, which have been extensively studied in the commutative algebra community.

Ayah Almousa
University of Minnesota - Twin Cities
almou007@umn.edu

Anton Dochtermann
Texas State University
dochtermann@txstate.edu

Ben Smith
University of Manchester
Heilbronn Institute for Mathematical Research
benjamin.smith-3@manchester.ac.uk

MS79

Viewing Graph Solvability

In structure-from-motion the viewing graph is a graph where vertices correspond to cameras and edges represent fundamental matrices. We provide a new formulation and an algorithm for establishing whether a viewing graph is solvable, i.e. it uniquely determines a set of projective cameras. Known theoretical conditions either do not fully characterize the solvability of all viewing graphs, or are exceedingly hard to compute for they involve solving a system of polynomial equations with a large number of unknowns. We show how to reduce the number of unknowns by exploiting the cycle consistency. We advance the understanding of the solvability by (i) finishing the classification of all previously undecided minimal graphs up to 9 nodes, (ii) extending the practical solvability testing up to minimal graphs with up to 90 nodes, and (iii) definitely answering an open research question by showing that the finite solvability is not equivalent to the solvability. Finally, we present an experiment on real data showing that unsolvable graphs are appearing in practical situations.

Federica Arrigoni
Politecnico di Milano
federica.arrigoni@polimi.it

Andrea Fusiello
University of Udine
andrea.fusiello@uniud.it

Elisa Ricci
University of Trento & Fondazione Bruno Kessler
e.ricci@unitn.it

Tomas Pajdla
Czech Technical University in Prague
pajdla@cvut.cz

MS79

Recognizing the Shape of a Point Configuration from Noisy Observations

Let $p_1, \ldots, p_k \in \mathbb{R}^d$ be a generic configuration of points. Previous work with G. Kemper showed that the multiset of pairwise distances between the points determines $p_1, \ldots, p_k$ up to an unknown rigid motion. In this work, we generalize this result to the case where the points are measured under noisy conditions. We view the noisy point measurements as i.i.d. samples from a mixture of k Gaussians whose means are at $p_1, \ldots, p_k$, respectively. Let $\Delta = \|x_1 - x_2\|^2$ be the square distance between two samples x_1, x_2 from the Gaussian mixture, and denote by $r(\Delta)$ the probability density function of Δ. We explore the question: under what circumstances does $r(\Delta)$ uniquely determine the Gaussian mixture, up to an unknown rigid motion? The question is rephrased using polynomial equations involving the moments of $r(\Delta)$ and the parameters of the Gaussian mixture. The number of real positive solutions for these equations corresponds to the number of possible Gaussian mixture reconstructions, up to a rigid motion. This is work in collaboration with Kindyl King and Uli Walther.

Mireille Boutin
Purdue University
U.S.
mboutin@purdue.edu

Kindyl King, Uli Walther
Purdue University
king487@purdue.edu, walther@purdue.edu

MS79

The Geometry of Rank Drop in Two-View Image Reconstruction

Given 6 points $(x_i, y_i) \in \mathbb{P}^2 \times \mathbb{P}^2$ we characterize rank deficiency of the 6×9 Z matrix with rows $x_i^\top \otimes y_i^\top$ in terms of the geometry of the point configurations $\{x_i\}$ and $\{y_i\}$. This rank drop locus is captured by the classical theory of cubic surfaces.

Erin Connelly
University of Washington
erin96@uw.edu

Sameer Agarwal
Google Inc
sameeragarwal@google.com

Alperen Ergur
University of Texas, San Antonio
alperen.ergur@utsa.edu

Rekha Thomas
University of Washington
rrthomas@uw.edu

MS79

Using Monodromy to Recover Symmetries of Polynomial Systems

Galois/monodromy groups attached to parametric systems of polynomial equations provide a method for detecting the existence of symmetries in solution sets. Beyond the question of existence, one would like to compute formulas for these symmetries, towards the eventual goal of solving the systems more efficiently. I will describe one possible approach to this task using numerical homotopy continuation and multivariate rational function interpolation. I will illustrate this approach on practical examples of minimal problems in computer vision. This is joint work with Timothy Duff, Tomas Pajdla and Margaret Regan.

Viktor Korotynskiy
CIIRC, CTU in Prague
korotynskiy.viktor@gmail.com

Timothy Duff
University of Washington
Seattle, WA
timduff@uw.edu

Tomas Pajdla
Czech Technical University in Prague
pajdla@cvut.cz

Margaret H. Regan
Duke University
Durham, NC USA
mregan@math.duke.edu

MS80

Revisiting Cycles of Pairing-Friendly Elliptic Curves

In this talk, I will present our work on 2-cycles of pairing-friendly elliptic curves of prime order. First, I will explore families of curves parameterized by polynomials, which is the only known method to produce prime-order curves, and then I will show that no 2-cycles can arise from the known families, except for those cycles already known. A consequence of this result is that it seems very unlikely that new pairing-friendly 2-cycles can be found, which has a direct impact on recursive composition of pairing-based proof systems.

Marta Bellés Muñoz
Dusk Network
Pompeu Fabra University, Barcelona, Spain
marta@dusk.network

MS80

A Short-List of Pairing-Friendly Curves Resistant to the Special Tnfs at 192-Bit Security Level

Selecting optimal elliptic curves for pairing-related scenarios is a complicated process. From a security point of view, one needs to consider the improved attacks of Kim-Barbulescu reducing the security level of extension fields of composite degree, hence forcing the scaling of the elliptic curve parameters so that the desired security level in the pairing-groups G_1, G_2, G_T is preserved. From a performance perspective, depending on the application, different operations in G_1, G_2 and G_T, such as the pairing computation, cofactor clearing, subgroup membership testing, or hashing to G_1, G_2, affect the efficiency of pairing-based protocols. For 128-bit security level, the BLS12 pairing-friendly elliptic curves dominate in application domains providing the best balance in terms of performance and security. For 192-bit security the situation is currently unclear. In this talk we go through new and existing TNFS-secure elliptic curves at 192-bit security, with embedding degrees from 16 to 28. We present a theoretical comparison of these curves in terms of performance and using SageMath and Magma prototype implementations for estimating cost in terms of multiplications over GF(p). Based on this theoretical comparison, we identify the most prominent pairing-friendly curves which are benchmarked in RELIC-optimized implementation considering not only the pairing computation itself, but also different group operations in the pairing groups G_1, G_2 and G_T.

Georgios Fotiadis
Université du Luxembourg
georgios.fotiadis@uni.lu

MS80

X-Superoptimal Pairings on Some Elliptic Curves with Odd Prime Embedding Degrees

The choice of the elliptic curve for a given pairing based protocol is primordial. For many cryptosystems based on pairings such as group signatures and their variants (EPID, anonymous attestation, etc) or accumulators, operations in the first pairing group $\mathbb{G}$ of points of the elliptic curve is more predominant. At 128-bit security level two curves $BW13-P310$ and $BW19-P286$ with odd embedding degrees 13 and 19 suitable for super optimal pairing have been recommended for such pairing based protocols . But a prime embedding degree ($k = 13; 19$) eliminates some important optimisation for the pairing computation. However The Miller loop length of the superoptimal pairing is the half of that of the optimal ate pairing but involve more exponentiations that affect its efficiency. In this work, we successfully develop methods and construct algorithms to efficiently evaluate and avoid heavy exponentiations that affect the efficiency of the superoptimal pairing. This leads to the definition of new bilinear and non degenerate pairing on $BW13-P310$ and $BW19-P286$ called x-superoptimal pairing where its Miller loop is about 15.3% and 39.8% faster than the one of the optimal ate pairing previously computed on $BW13-P310$ and $BW19-P286$ respectively.

Emmanuel Fouotsa
Université de Bamenda, Cameroon
emmanuelfouotsa@yahoo.fr

MS80

An Algebraic Point of View on the Generation of Pairing-Friendly Curves

In 2010, Freeman Scott and Teske published a well-known taxonomy compiling the best known families of pairing-friendly elliptic curves. Since then, the research effort mostly shifted from the generation of pairing-friendly curves to the improvement of algorithms or the assessment of security parameters to resist the latest attacks on the discrete logarithm problem. Consequently, very few new families were discovered. However, the need of pairing-friendly curves of prime order in some new applications such as SNARKs has reignited the interest in the generation of pairing-friendly curves, with hope of finding families similar to the one discovered by Barreto and Naehrig. Building on the work of Kachisa, Schaefer and Scott, we show that some elements of extensions of cyclotomic field have a higher probability of generating a family of pairing friendly curves. We present a general framework which embraces the KSS families and many of the other families in the taxonomy paper, and provide an open-source SageMath implementation of our technique. We finally introduce a new family with embedding degree $k = 20$ which we estimate to provide a faster pairing compared to KSS16 and KSS18 at the 192-bit security level.

Jean Gasnier
Université de Bordeaux, France
jean.gasnier@u-bordeaux.fr

Aurore Guillevic
Inria Nancy Grand Est
aurore.guillevic@inria.fr

MS81

Introductory Talk

Finite fields play a crucial role in cryptography and coding theory. This talk aims to provide an overview of the different topics and techniques presented by the speakers.

Daniele Bartoli
Department of Mathematics - University of Perugia
daniele.bartoli@unipg.it

MS81

Norm-trace Lifted Codes

Hermitian-lifted codes were introduced in 2021 by Lpez, Malmskog, Matthews, Piero-Gonzlez and Wootters. Hermitian-lifted codes are a family of evaluation codes in which coordinates correspond to affine points on the Hermitian curve and codewords are given by evaluating a special set of functions which are low degree polynomials when restricted to lines intersecting the curve. Local recovery of erasures is accomplished via repair groups which are the intersections of lines through that point and the curve itself, yielding high availability and positive code rate. In this talk, we consider an analogous code design using instead the norm-trace curve. We explore settings in which the norm-trace curves yield codes are easier to define and provide some potential advantages in terms of locality, meaning the number of symbols required to recover another, or alphabet size.

Gretchen Matthews
Virginia Tech, U.S.
gmatthews@vt.edu

MS81

Maximum Weight Codewords in Rank Metric Codes and Linear Sets

For an $\mathbb{F}_{q^m}$-linear non-degenerate rank metric code $\mathcal{C}$ in $\mathbb{F}_{q^m}^n$, define $M(\mathcal{C})$ as the number of codewords in $\mathcal{C}$ having weight $\min\{m, n\}$. In this talk, we investigate the following two problems:

- To determine upper and lower bounds on $M(\mathcal{C})$.
- To characterize the extremal cases in the obtained bounds on $M(\mathcal{C})$.

The main tools used are linear sets, which are point sets in a projective space $\mathrm{PG}(V, \mathbb{F}_{q^n})$ defined by an $\mathbb{F}_q$-subspace of V. We use old and new bounds regarding the size and the weight distribution of linear sets, to obtain the desired bounds. Then we analyze the case of equality in the lower and upper bounds on $M(\mathcal{C})$ by capturing the geometry of these codes. We will see that the codes attaining these bounds are strongly related to scattered linear sets and hence to MRD codes and linear sets having minimum size.

Olga Polverino
University of Campania
olga.polverino@unicampania.it

Paolo Santonastaso
University of Caserta
paolo.santonastaso@unicampania.it

Ferdinando Zullo
Università degli Studi della Campania
ferdinando.zullo@unicampania.it

MS81

Algebraic Geometric Methods in Coding Theory and Cryptography: Some Recent Results

In the last decades, Algebraic Geometry over finite fields has been used to investigate a wide variety of objects closely related to Galois Geometry, Coding Theory and Cryptography. Among such objects, we mention MRD codes and highly non-linear functions. In this talk, we will show some recent results obtained using algebraic geometric methods. In this context, a key role is played by a careful analysis of the irreducible components of certain algebraic varieties, together with Hasse-Weil type theorems.

Marco Timpanella
University of Perugia
marco.timpanella@unipg.it

MS82

On Complete m-Arcs from Algebraic Curves

Let m and k be two positive integers and q be an odd prime power. Let $PG(2, q)$ be the set of $\mathbb{F}_q$-points of the projective plane. A (k, m)-arc $\mathcal{A}$ in $PG(2, q)$ is a set of k points such that there are no $m+1$ points that are collinear but there exist m collinear points. For fixed m, q, we have that the set $\mathcal{A}_m(q)$ of all m-arcs in $PG(2, q)$ is partially ordered by inclusion. A complete m-arc is a maximal element in $\mathcal{A}_m(q)$, i.e. it is an m-arc that is not contained in a strictly larger m-arc. The purpose of this talk is to provide a general theory to construct families of complete m-arcs arising from curves that satisfy explicit and generic geometric conditions. This is a joint work with Giacomo Micheli.

Luca Bastioni, Giacomo Micheli
University of South Florida
lbastioni@usf.edu, gmicheli@usf.edu

MS82

On the Sunflower Bound for k-spaces Pairwise Intersecting in a Point

Let $\mathrm{PG}(n, q)$ be the projective space of dimension n over the finite field of order q. We look at families of k-spaces that pairwise intersect in *exactly* a t-space. These families can also be described within the context of subspace codes. We refer to them as *t-intersecting constant dimension codes*, or abbreviated *SCID's*. The classical example of a t-intersecting constant dimension code is the set of k-spaces pairwise intersecting in a fixed t-space α, which is called a *sunflower* through α. Within the theory on t-intersecting constant dimension codes, it is a known result that large t-intersecting constant dimension codes are equal to sunflowers. More precisely, the following result is known. Let C be a t-intersecting constant dimension code of k-spaces in $\mathrm{PG}(n, q)$, where

$$|C| > \left(\frac{q^{k+1} - q^{t+1}}{q-1}\right)^2 + \left(\frac{q^{k+1} - q^{t+1}}{q-1}\right) + 1,$$

then C is a sunflower. This lower bound is called the *sunflower bound* and it is generally believed that the lower bound of the preceding theorem is too large. This motivates the research to improve this lower bound. In this talk, I will present an improvement on the sunflower bound for k-spaces, pairwise intersecting in a projective point. This is a joint work with Aart Blokhuis and Maarten De Boeck.

Jozefien D'haeseleer
Ghent University
jozefien.dhaeseleer@ugent.be

MS82

Spatially Coupled LDPC Codes from Finite Geometries

Spatially coupled LDPC (SC-LDPC) codes are graph-based codes notable for their decoding threshold and performance. Their construction may be viewed in several ways, including replicating a small Tanner graph for a code and “spreading edges so that the copies interact, or via algebraic graph lifts. In this talk, we provide some general distance bounds of SC-LDPC codes given properties of their base Tanner graph. In particular, we present an explicit construction of SC-LDPC codes based on finite geometries and prove results about the minimum distance of these codes. We show that with the right edge spreading, these codes can attain the maximum distance possible for a spatially coupled code given the initial base graph.

Emily McMillon
Rice University

emily.mcmillon@rice.edu

Christine A. Kelley, Tefjol Pllaha
University of Nebraska-Lincoln
ckelley2@unl.edu, tefjol.pllaha@unl.edu

MS82

Optimal Small-Set Expanders and Their Applications

Let t, d be positive integers and let α be a real number. A left-regular bipartite graph G of degree d is called a (t, α)-*small-set-expander* if every subset $X \subseteq L$ of size at most t has at least $\alpha|X|$ neighbors. We define the t-th expansion constant $\alpha_G(t)$ of G as the largest α such that G is a (t, α) small-set-expander. Note that a sequence $(G_n)_{n\in\mathbb{N}}$ of (t, α) small-set expanders is not a sequence of (γ, α) expanders because the fraction $\gamma := t/|L|$ of left vertices we consider is not kept constant and is even allowed to vanish asymptotically, making it easier to build families of small-set expander graphs. The aim of this article is to provide constructions of bipartite graphs which are provably optimal small-set expanders and to show that they lead to extremely useful codes. To illustrate their applications we propose a novel McEliece type code-based cryptographic scheme with excellent security guarantees as well as fast encryption and decryption procedures. These results are ongoing joint work with T. Bogart and V. Gauthier

Mauricio Velasco
Universidad de los Andes
mvelasco@uniandes.edu.co

Tristram C. Bogart
San Francisco State University
tcbogart@gmail.com

Valerie Gauthier
Universidad de los Andes
ve.gauthier@uniandes.edu.co

MS83

The Christoffel Function and Its Connection with Positivity Certificates

We introduce the Christoffel function (CF), a well-known tool in theory of approximation and orthogonal polynomials. We will briefly describe how the CF turns out to also provide a quite easy-to-use tool to help solve interesting problems in data analysis (e.g., outlier detection, support inference, density approximation, classification). We will also discuss some (in the author's opinion surprising) links with seemingly unrelated topics, like e.g., certificates of positivity in real algebraic geometry, equilibrium measure of compact sets, polynomial Pell's equation, and duality in polynomial optimization.

Jean B. Lasserre
LAAS CNRS and Institute of Mathematics
lasserre@laas.fr

MS83

Path Signature and Volume of Convex Hulls of Curves

How can one compute the volume of the convex hull of a curve? I will try to answer this question, for special families of curves. This generalizes a previously known integral formula. Our methods involve approximating the curve with cyclic polytopes and using the tool of ”path signature”. I will give a geometric interpretation of this volume formula in terms of lengths and areas, and conclude with examples and an open conjecture. This is a joint work with Carlos Amndola and Darrick Lee (arXiv:2301.09405).

Chiara Meroni
ICERM, Brown University
chiara_meroni@brown.edu

MS83

Nonnegative Polynomials Without Hyperbolic Certificates of Nonnegativity

If a multivariate polynomial is a sum of squares then it is nonnegative. However, it is well known that there are nonnegative polynomials that are not sums of squares. Recently, other strategies for certifying the nonnegativity of homogeneous multivariate polynomials have been proposed based on the theory of hyperbolic polynomials. These hyperbolic certificates contain sum-of-squares certificates as special cases. In this talk I will discuss the question of whether there exist nonnegative polynomials that do not have such hyperbolic certificates of nonnegativity.

James Saunderson
Department of Electrical and Computer Systems Engineering
Monash University
james.saunderson@monash.edu

Brian Ng
Monash University
hin.ng@monash.edu

MS83

The Lasserre Hierarchy for Equiangular Lines with a Fixed Angle

The equiangular lines problem asks for the maximum number of lines through the origin in n-dimensional Euclidean space such that the angle between any pair of lines is the same. When fixing the angle, this maximum is known to be linear in the dimension, but previously computed SDP bounds fail to recover this behavior. In this talk, I will discuss the Lasserre hierarchy for this problem. I will show how we can compute the second and third levels (the first level is identical to the Delsarte LP bound) by using a connection between representations of the general linear group and invariant subspaces of representations of the orthogonal group. Then I will explain how we can asymptotically analyze the resulting SDP bounds, and use this to prove the Lasserre hierarchy gives linear bounds in the dimension for several angles.

David de Laat
Delft University of Technology
d.delaat@tudelft.nl

Fabricio Machado
Universidade de São Paulo
fabcm1@gmail.com

Willem De Muinck Keizer
TU Delft

willemdmk@gmail.com

MS84

Polynomial Conditions of Qualitative Properties of Biological Interaction Networks

The dynamics of biochemical reaction networks can be described by ODEs with polynomial right hand side. Due to high measurement uncertainty, few experimental repetitions and a limited number of measurable components, parameters are subject to high uncertainty and can vary in large intervals. One therefore effectively has to study families of parametrized polynomial ODEs. In this presentation families are considered where the steady state variety can be parameterized by monomials. I discuss how one can expolit these parameterizations to derive polynomial conditions for the occurence of multistationarity or Hopf bifurcations.

Carsten Conradi
HTW Berlin
carsten.conradi@htw-berlin.de

MS84

Improved Steady State Bounds with Tropical and Toric Methods

One of the central questions in reaction network theory is how the number of positive steady states for a given network varies with the rate constants and total concentrations. An important subproblem is finding the steady state degree (SSD), i.e. the maximal number of steady states over $\mathbb{C}^*$, which is needed for fast and certifiable numerical computations of the steady states. In the first part of the talk, I will discuss new techniques for determining the SSD, by expressing it as a certain tropical intersection number, which we compute for many realistically sized networks (with ¡50 species) through a newly developed algorithm, based on previous work by Helminck and Ren. We also give a sufficient condition for when the SSD can be computed much faster as the mixed volume of a polynomial system consisting of appropriately chosen steady state equations and conservation laws – despite these equations having dependencies between the coefficients, which turn them into a strict subfamily of the family with fully free coefficients considered in the BKK theorem. In the second part of the talk, I will discuss the special case when the positive part of the steady state variety is toric (in the sense that it admits a monomial parametrization) for all rate constants, which often makes it possible to give faster and sharper bounds over $\mathbb{R}_{>0}$ than the SSD. This is based on a combination of joint works with Feliu, Helminck, Ren, Schrter and Telek.

Oskar Henriksson
University of Copenhagen
oskar.henriksson@math.ku.dk

MS84

The Disguised Toric Locus and Affine Equivalence of Reaction Networks

Under the assumption of mass-action kinetics, a dynamical system may be induced by several different reaction networks and/or parameters. It is therefore possible for a mass-action system to exhibit complex-balancing dynamics without being weakly reversible or satisfying toric constraints on the rate constants; such systems are called disguised toric dynamical systems. We show that the parameters that give rise to such systems are preserved under invertible affine transformations of the network. We also consider the dynamics of arbitrary mass-action systems under affine transformations, and show that there is a canonical bijection between their sets of positive steady states, although their qualitative dynamics can differ substantially. This is joint work with Sabina J. Haque, Matthew Satriano and Polly Y. Yu.

Sabina Haque
Harvard University
sabina_haque@fas.harvard.edu

Matthew Satriano
Department of Pure Mathematics, University of Waterloo, Cana
msatriano@uwaterloo.ca

Miruna-Stefana Sorea
SISSA, Trieste and RCMA ULBS
SISSA, Trieste and RCMA ULBS
miruna.stefana.sorea2019@gmail.com

Polly Yu
Harvard University
pollyyu@fas.harvard.edu

MS84

Complex Balanced Distributions

This talk is concerned with complex balanced reaction network and their stochastic behavior, in particular the existence and form of stationary distributions; the analogue of equilibrium points in the context of deterministic dynamics. Specifically, we consider reaction networks modeled by Continuous Time Markov Chains and characterize complex balanced distributions of reaction networks with arbitrary transition functions through conditions on the cycles of their corresponding reaction digraphs. The proof works by constructing a dynamically equivalent reaction network with disjoint cycles. We further derive a sufficient condition for the existence of a complex balanced distribution, and give precise conditions on when it is necessary. The sufficient condition holds for mass-action kinetics or if the digraph consists of only cyclic connected components. Hence, we fully characterize the existence and form of complex balanced distributions. Furthermore, we outline the relationship to reaction networks modeled by ODE systems and discuss how similar results might be obtained in this case. The work is joint with Panqiu Xia and Linard Hoessly.

Carsten Wiuf
University of Copenhagen
wiuf@math.ku.dk

MS85

Randomly Updated Markov Bases Algorithm (RUMBA) for Sampling Lattice Points in a Polytope

Fiber sampling often uses MCMC methods that traverse edges in a connected fiber graph given by moves in a Markov basis. These methods are limited by the complexity of computing the basis, such that for large fibers it is infeasible to compute every move required for connectivity, and dynamic computation is needed instead. Additionally, bottlenecks can occur in chains on graphs with low connectivity. We develop a biased sampling algorithm for sampling a fiber from an easy-to-compute lattice basis. We showcase its performance on some known examples whose Markov bases fiber graphs have known bottlenecks. The talk will discuss the notion of a fiber discovery rate, some background on mixing time and Markov chains, and present the idea behind this Bayesian biased sampler of points in a fiber. Joint work with Sonja Petrovic.

Miles Bakenhus
Illinois Institute of Technology
mbakenhus@hawk.iit.edu

Sonja Petrovic
Illinois Institute of Technology, Department
of Applied Mathematics, Chicago IL 60616
sonja.petrovic@iit.edu

MS85

H-Representations of Characteristic Imset Polytopes via Quasi-Independence Gluing

Characteristic imsets are 0-1 vectors which correspond to Markov equivalence classes of directed acyclic graphs. The study of their convex hull, named the characteristic imset (CIM) polytope, has led to new and interesting geometric perspectives on the important problem of causal discovery. In this talk we'll focus on the sub-polytope which whose vertices correspond to all DAGs with a fixed skeleton. Recent work by the latter four authors shows that the vertices of this polytope can be obtained by a new operation called quasi-independence gluing which generalizes Sullivant's toric fiber product. In this talk, we show that this structure can be used to iteratively build an H-representation of the CIM polytope of a tree from that of smaller trees.

Jane Coons
St John's College, University of Oxford
jane.coons@sjc.ox.ac.uk

Benjamin Hollering
Max Planck Institute for Mathematics in the Sciences
benhollering@gmail.com

Joseph Johnson
North Carolina State University
jwjohns5@ncsu.edu

Irem Portakal
Technical University of Munich
irem.portakal@tum.de

Liam Solus
KTH Royal Institute of Technology
solus@kth.se

MS85

Facets of Correlation Polytopes

Hierarchical models are statistical models that describe dependence among discrete random variables. For binary hierarchical models there is an associated correlation polytope, whose dilates contain the sufficient statistics of the model (up to a change of coordinate). We describe facet defining inequalities for a special class of correlation polytopes.

Joseph Johnson, Seth Sullivant
North Carolina State University
jwjohns5@ncsu.edu, smsulli2@ncsu.edu

MS85

Toric and Non-Toric Staged Trees and Bayesian Nets

Staged trees and Bayesian networks are discrete statistical models with a graphical representation, and can also be described as algebraic varieties. In this talk we will study connections between the graphical representation and algebraic properties of the corresponding vanishing ideals. In particular we would like to understand which graphs give rise to toric ideals, and which do not, when allowing linear change of coordinates.

Lisa Nicklasson
Università di Genova
nicklasson@dima.unige.it

MS86

Using Betti Tables As Tensor Invariants with a View Toward Complexity

A three place tensor may be associated with the subspace of matrices which are contractions of the first factor, and the data of this subspace determines the original tensor up to isomorphism. To a subspace of square matrices containing an invertible element, one can associate a reciprocal variety, consisting of the closure of the matrix inverses of invertible matrices from the subspace. Discrete invariants of the reciprocal variety are isomorphism invariants of the tensor they arise from. I discuss some of these invariants, particularly values of the Hilbert function and entries of the Betti table of the reciprocal variety, and indicate where they have relation to the more classical tensor complexity invariants of rank and border rank.

Austin Conner
Texas A&M Univeristy
austin.conner@uni-konstanz.de

Hanieh Keneshlou
University of Konstanz
hanieh.keneshlou@uni-konstanz.de

MS86

Condition Numbers of Tensor Factorisations

Tensor factorisations, such as the Tucker or tensor train decomposition are underdetermined polynomial systems. That is, a given tensor has infinitely many equivalent decompositions. If a measured tensor is corrupted by noise, one should ask whether the noisy tensor has any decomposition that is close to a decomposition of the noiseless tensor. The answer to this question depends on the *condition number*, which I will introduce in sufficient generality to handle underdetermined systems. Then, I will show how the condition number of a Tucker decomposition can be computed in terms of the higher-order singular value decomposition.

Nick Dewaele
KU Leuven, Belgium

nick.dewaele@kuleuven.be

MS86

Phylogenetic Ideals Beyond Equivariant Models

Evolutionary models can be seen as algebraic varieties given by relations among the entries of the tensor of joint probabilities of all possible observations at the leaves of a phylogenetic tree. In this talk we will discuss the mathematical properties of a phylogenetic substitution model for nucleotides proposed by Tamura and Nei (TN93). TN93 generalizes well-known models like Jukes-Cantor or Kimura 2-parameters in the sense that allows for any arbitrary non-uniform stationary distribution π. We will compute phylogenetic invariants (i.e. generators of the vanishing ideal) of phylogenetic trees with a small number of leaves and obtain local complete intersections at points of biological interest.

Roser Homs Pons
Centre de Recerca Matemàtica, Spain
rhoms@crm.cat

Marta Casanellas
Departament de Matematiques
Universitat Politècnica de Catalunya
marta.casanellas@upc.edu

Angelica Torres
Centre de Recerca Matemàtica
atorres@crm.cat

Jesús Fernández Sánchez
Universitat Polytecnica de Catalunya
Department of Mathematics
jesus.fernandez.sanchez@upc.edu

MS87

Toward Automatically Computed Assemblable Singular Algebraic Surfaces

Algebraic surfaces are beautiful. They show up on covers of math journals, posters. There are websites full of them, including Herwig Hauser's gallery of Singular Algebraic Surfaces, my primary inspiration for this project. Maximally singular surfaces are particularly interesting; Barth's Sextic is a notable example. And the plaster galleries found at a number of universities are a testament to their ongoing power to enthrall and fascinate. My work with algebraic surfaces has tended toward plastic renditions fabricated by a 3d printer, powered by an algorithm called Numerical Real Cellular Decomposition as implemented in `bertini_real`. My aspirational goal is an automated suite of software for ready-to-print model creation for surfaces with arbitrary singularity structures, in any number of dimensions. A number of barriers lie in the way. This talk will discuss some of those barriers, and my progress in overcoming them. In particular, I will talk about a general plug-and-socket modality for nodal singularities that allows for snap-together assembly, and an open-to-me problem about orientation of the joints. I will also discuss issues in adaptive triangulation refinement in N dimensions for $N > 3$, and challenges in solidification around singularities.

Silviana Amethyst, Morgan Fiebig, Caden Joergens
University of Wisconsin Eau Claire
silvianaamethyst@gmail.com, fiebigm8842@uwec.edu, joergenc9157@uwec.edu

MS87

An Algebraic Approach to Understanding Long Branch Attraction in Phylogenetics

Reconstructing and understanding the Tree of Life is a central question biology, and while genetic data has proven to be an essential tool in studying the evolutionary relationships between living organisms, the 'best' way to use such data to evolutionary trees is a major area of study. One commonly-used approach is *maximum likelihood*: one first assumes that the gene sequences evolved according to some model of evolution parameterized by an evolutionary tree parameter (representing a hypothesis about the species' evolutionary histories). Then, given some observed data, one can estimate the tree which maximizes the likelihood of the data under the model. However, sometimes this method fails catastrophically in ways that are not yet fully understood. In this talk, I will present ongoing work with Jose Rodriguez investigating *Long Branch Attraction* (LBA), a phenomenon in which maximum likelihood incorrectly infers distantly related taxa to be much more closely related than they really are. We present an approach using phylogenetic invariants and homotopy continuation to numerically solve for the MLE in the simplest case of a four leaf tree, and use this to establish criteria for LBA susceptibility using Likelihood Ratios.

Max Bacharach
University of Wisconsin Madison
bacharach@wisc.edu

MS87

Polyhedral Homotopy for Solving Deficient Polynomial Systems

Deficient polynomial systems are systems whose complex root counts are strictly lower than a given sharp upper bound on the root counts. In this talk, we focus on systems that are deficient with respect to their Bernshtein-Kushnirenko-Khovanskii bound. Solving deficient polynomial systems using homotopy methods introduces ”divergent paths” that are not only wasteful but also numerically ill-conditioned. We explore a few computationally cheap modifications to the polyhedral homotopy method of Huber and Sturmfels that can help us to solve deficient polynomial systems while avoiding divergent paths.

Tianran Chen
Auburn University Montgomery
ti@nranchen.org

Julia Lindberg
University of Texas-Austin
julia.lindberg@math.utexas.edu

MS87

Benefits and Drawbacks of Singularities in Applications

Many applications can be modeled using parameterized systems of polynomials. Since such polynomial models typically have singularities, one can recognize both benefits and drawbacks of singularities. For example, the number of real solutions can change at singularities, which can be beneficial or detrimental depending on the application. This talk will explore his dichotomy through applications in kinematics and biological modeling.

Jonathan Hauenstein
University of Notre Dame
Dept. of App. Comp. Math. & Stats.
hauenstein@nd.edu

MS88

Crystallographic Symmetries in Trigonometric Optimization

Trigonometric polynomials are usually defined on the lattice of integers. In this talk, we consider the larger class of weight and root lattices with crystallographic symmetry. We give a new approach to minimize trigonometric polynomials, which are invariant under the associated reflection group. The invariance assumption allows us to rewrite the objective function in terms of generalized Chebyshev polynomials. The new objective function is defined on a compact basic semi-algebraic set, so that we can benefit from the rich theory of polynomial optimization. We present an algorithm to compute the minimum: Based on the Hol-Scherer Positivstellensatz, we impose matrix-sums of squares conditions on the objective function in the Chebyshev basis. The degree of the sums of squares is weighted, defined by the root system. Increasing the degree yields a converging Lasserre-type hierarchy of lower bounds. This builds a bridge between trigonometric and polynomial optimization, allowing us to compare with existing techniques. The presented results are based on joint work with Evelyne Hubert (Inria d'Université Cote d'Azur), Philippe Moustrou (Université Toulouse Jean Jaures) and Cordian Riener (UiT The Arctic University).

Tobias Metzlaff
University of Kaiserslautern-Landau
tobias.metzlaff@rptu.de

MS88

Improved Effective Lojasiewicz Inequality and Applications

Let R be a real closed field. Given a closed and bounded semi-algebraic set $A \subset \mathrm{R}^n$ and semi-algebraic continuous functions $f, g : A \to \mathrm{R}$, such that $f^{-1}(0) \subset g^{-1}(0)$, there exist N and $c \in \mathrm{R}$, such that the inequality (Lojasiewicz inequality) $|g(x)|^N \leq c \cdot |f(x)|$ holds for all $x \in A$. Here, we consider the case when A is defined by a quantifier-free formula with atoms of the form $P = 0, P > 0, P \in F$ for some finite subset of polynomials $F \subset \mathrm{R}[X_1, \ldots, X_n]_{\leq d}$, and the graphs of f, g are also defined by quantifier-free formulas with atoms of the form $Q = 0, Q > 0, Q \in G$, for some finite set $G \subset \mathrm{R}[X_1, \ldots, X_n, Y]_{\leq d}$. We prove that the Lojasiewicz exponent N in this case is bounded by $(8d)^{2(n+7)}$. Our bound depends on d and n, but is independent of the combinatorial parameters, namely the cardinalities of F and G. We exploit this fact to improve the best known error bounds for polynomial and non-linear semi-definite systems.

Saugata Basu
Department of Mathematics, Purdue University
sbasu@purdue.edu

Ali Mohammad Nezhad
Department of Math Sciences, Carnegie Mellon University
anezhad@andrew.cmu.edu

MS88

Effective PositivStellensatz and Polynomial Optimization

Polynomial optimization on a semi-algebraic set S can be reformulated into a convex optimization program, which involves the convex cone of positive polynomials on S. Its dual involves the cone of moments of probability measures. As cones of positive polynomials are difficult to describe effectively, hierarchies of tractables cones such as sum-of-squares cones also known as Lasserre's hierarchy have been proposed to approximate them. The efficiency of the approach depends on the properties of representation of strictly positive polynomials in these cones, known as the PositivStellensatz. We will present new results about the Effective PositivStellensatz, regarding the degree and the norm of representations of the strictly positive polynomials on S for different convex cone hierarchies, including SOS hierarchies.

Lorenzo Baldi
Sorbonne Université, CNRS
PolSys - Polynomial Systems LIP6, Paris, France
lorenzo.baldi@inria.fr

Bernard Mourrain
INRIA Sophia Antipolis
Bernard.Mourrain@inria.fr

MS88

Linear Slices of Hyperbolic Polynomials and Positivity of Symmetric Polynomial Functions

A real univariate polynomial of degree n is called hyperbolic if all of its n roots are on the real line. Such polynomials appear quite naturally in different applications, for example, in combinatorics and optimization. The focus of this talk are families of hyperbolic polynomials which are determined through k linear conditions on the coefficients. The coefficients corresponding to such a family of hyperbolic polynomials form a semi-algebraic set which we call a *hyperbolic slice*. The set of hyperbolic polynomials is naturally stratified with respect to the multiplicities of the real zeros and this stratification induces also a stratification on the hyperbolic slices. Our main focus here is on the *local extreme points* of hyperbolic slices, i.e., the local extreme points of linear functionals, and we show that these correspond precisely to those hyperbolic polynomials in the hyperbolic slice which have at most k distinct roots and we can show that generically the convex hull of such a family is a polyhedron. Building on these results, we give consequences of our results to the study of symmetric real varieties and symmetric semi-algebraic sets. Here, we show that sets defined by symmetric polynomials which can be expressed sparsely in terms of elementary symmetric polynomials can be sampled on points with few distinct coordinates. This in turn allows for algorithmic simplifications, for example,to verify that such polynomials are non-negative.

Robin Schabert
UiT - The Arctic University of Norway
robin.schabert@uit.no

MS89

Towards the Function Space for Two-Loop Six-

Particle Feynman Integrals

Scattering amplitudes are central objects in quantum field theory as they serve as a bridge between theory and experiments. The state-of-the-art in current two-loop QCD amplitude calculations is at five-particle scattering. In contrast, very little is known at present about two-loop six-particle scattering processes. In order to compute these scattering amplitudes we need to compute Feynman integrals appearing in them. Since computing the two-loop six-particle processes requires the knowledge of the corresponding one-loop amplitudes to higher orders in the dimensional regulator, we will first take a look at analytic results for the one-loop hexagon integrals obtained via the differential equation method. Furthermore, we will discuss the current status of the full two-loop computation.

Antonela Matijasic
Max Planck Institute for Physics
amatijas@mpp.mpg.de

MS89

Resultants on $M_{\{0,n\}}$

Resultants is a central tool in elimination theory: they are used to solve polynomial systems, to determine existence of solutions, or to reduce a given system to a smaller one. The classical theory of resultants considers homogeneous polynomial systems on projective spaces. In recent years, a lot of classical theory was generalised to the case where projective space is replaced by an arbitrary irreducible variety X and homogeneous polynomials are replaced by sections of line bundles on X. In my talk I will first briefly recall the theory of generalised resultants. Then, motivated by scattering equations of CachazoHeYuan, I will specialise to the case of resultants of tautological line bundles on $M_{\{0,n\}}$

Leonid Monin
EPFL
leonid.monin@gmail.com

Simon Telen
MPI Leipzig
simon.telen@mis.mpg.de

MS89

D-Module Techniques for Feynman Integrals

Feynman integrals are solutions to linear partial differential equations with polynomial coefficients. Using a triangle integral with general exponents as a case in point, we compare D-module methods to dedicated methods developed for solving differential equations appearing in the context of Feynman integrals, and provide a dictionary among them. In particular, we implement an algorithm due to Saito, Sturmfels, and Takayama to derive canonical series solutions of regular holonomic D-ideals, and compare them to asymptotic series derived by the respective Fuchsian systems.

Lizzie Pratt
UC Berkeley
epratt@berkeley.edu

Johannes Henn
Max Planck Institute for Physics, Munich
henn@mpp.mpg.de

Anna-Laura Sattelberger
KTH Royal Institute of Technology
alsat@kth.se

Simone Zoia
University of Torino
simone.zoia@unito.it

MS90

The Tropical Nullstellensatz and Positivstellensatz for Sparse Polynomial Systems

Grigoriev and Podolskii (2018) have established a tropical analog of the effective Nullstellensatz, showing that a system of tropical polynomial equations is solvable if and only if a linearized system obtained from a truncated Macaulay matrix is solvable. They provided an upper bound of the minimal admissible truncation degree, as a function of the degrees of the tropical polynomials. We establish a tropical Nullstellensatz adapted to *sparse* tropical polynomial systems. Our approach is inspired by a construction of Canny-Emiris (1993), refined by Sturmfels (1994). This leads to an improved bound of the truncation degree, which coincides with the classical Macaulay degree in the case of $n+1$ equations in n unknowns. We also establish a tropical Positivstellensatz, allowing one to decide the inclusion of tropical basic semi-algebraic sets. This allows one to reduce decision problems for tropical semi-algebraic sets to the solution of systems of tropical linear equalities and inequalities. The later systems are known to be reducible to mean payoff games, which can be solved in practice, in a scalable way, by value iteration methods. We illustrate this approach by examples.

Antoine Béreau
INRIA and CMAP - École Polytechnique
antoine.bereau@inria.fr

Marianne Akian, Stephane Gaubert
INRIA and CMAP, Ecole Polytechnique
marianne.akian@inria.fr, stephane.gaubert@inria.fr

MS90

Computation of Mixed Volume – Current State and Research Directions

This talk surveys algorithmic approaches and complexity results for computing and for approximating mixed volume of a well-constrained system of convex polytopes. We recall the Bernstein-Khovanskii-Kushnirenko (BKK) bound on the number of isolated roots of well-constrained algebraic systems and we relate this bound to the multivariate Bzout bounds. We pay special attention to structured systems such as multi-homogeneous systems and propose a purely combinatorial method to derive closed-form bounds on BKK in certain cases. We also relate mixed volume to the permanent computation; the recent polynomial-time algorithm for computing a class of permanents raises interesting open questions for computing root bounds. Other algorithmic techniques for computing mixed volumes include the use of generating functions via MacMahons Master theorem, or orthogonal polynomials.

Ioannis Emiris
Athena Research Center

emiris@athenarc.gr

MS90
Computing Tropical Prevarieties

A tropical prevariety can be computed as the intersection of a finite number of tropical hypersurfaces each being the union of finitely many convex polyhedra. Experiments show that by dynamically decomposing the hypersurfaces into half open polyhedra, the enumeration tree can be made more narrow, allowing for larger examples to be computed. We report on progress on an exact arithmetic C++ implementation of such algorithm which is part of the gfan library. Its applications are in tropical algebraic geometry and in polynomial systems solving. In joint work with Leykin we use the implementation to reprove a generic finiteness result for relative equilibria in the Newtonian 5-body problem, first established by Albouy and Kaloshin in 2012.

Anders Jensen
Department of Mathematical Sciences
Aarhus University
jensen@math.au.dk

MS90
Introductory Lecture

Mixed Volume was introduced by Minkowski in connection to the geometry of convex bodies in 3-space. It applies to a tuple of convex bodies. The mixed volume V(A,A,A) specializes to the ordinary volume of A. If B is the 3-ball, V(A,A,B) gives the surface of the boundary (up to a constant), while V(A,B,B) is the total mean-curvature (also up to a constant). This geometric invariant is also related to the number of roots of a system of polynomial equations. Bernstein's Theorem states that the number of complex roots, with no coordinate equal to zero or infinity, of a generic system of n complex polynomials in n variables is (up to a constant) the mixed volume of the n-tuple with the convex hull of each support. Actually, this bound counts the number of roots in a certain toric variety One can also associate to each support a certain symplectic form in the toric variety. The mixed volume is the integral of the wedge product of the symplectic forms. But the expected number of root of real random polynomials can also be represented as a certain mixed volume. Since this will be the introductory lecture, I plan to survey the basic definitions and properties of the mixed volume, and maybe hint at the connections to other subjects in this conference.

Gregorio Malajovich
Universidade Federal do Rio de Janeiro
gregorio@im.ufrj.br

MS91
Moment Varieties of Linear Non-Gaussian Graphical Models

We study linear non-Gaussian graphical models from the perspective of algebraic statistics. These are acyclic causal models in which each variable is a linear combination of its direct causes and independent noise. The underlying directed causal graph can be identified uniquely via the set of second and third order moments of all random vectors that lie in the corresponding model. Our focus is on finding the algebraic relations among these moments for a given graph. We show that when the graph is a polytree these relations form a toric ideal. We construct explicit trek-matrices associated to 2-treks and 3-treks in the graph, whose entries are covariances and third order moments, and whose 2-minors define our model set-theoretically. Furthermore, we prove that their 2-minors generate the vanishing ideal of the model.

Carlos Améndola
Technical University of Berlin
amendola@math.tu-berlin.de

Mathias Drton
Technische Universität München, Germany
mathias.drton@tum.de

Alexandros Grosdos
Technical University of Munich
alex.grosdos@tum.de

Roser Homs Pons
Centre de Recerca Matemàtica, Spain
rhoms@crm.cat

Elina Robeva
University of British Columbia
erobeva@math.ubc.ca

MS91
Determinantal Varieties from Point Configurations on Hypersurfaces

Point configurations appear naturally in different contexts, ranging from the study of the geometry of data sets to questions in commutative algebra and algebraic geometry concerning determinantal varieties and invariant theory. In this talk, we bring these perspectives together: we consider the scheme $X_{r,d,n}$ parametrizing n ordered points in r-dimensional projective space that lie on a common hypersurface of degree d. We show that this scheme has a determinantal structure and, if $r > 1$, we prove that it is irreducible, Cohen-Macaulay, and normal. Moreover, we give an algebraic and geometric description of the singular locus of $X_{r,d,n}$ in terms of Castelnuovo-Mumford regularity and d-normality. This yields a complete characterization of the singular locus of $X_{2,d,n}$ and $X_{3,2,n}$. This is joint work with Han-Bom Moon and Luca Schaffler.

Alessio Caminata
University of Genova
caminata@dima.unige.it

MS91
Matrix Completion and the Algebraic Matroid of the Determinantal Variety

This talk will report progress on the characterization of the algebraic matroid of the classical determinantal variety; a problem related to low-rank matrix completion. A family of base sets of the matroid is presented, which characterizes the entire matroid in special cases. The proof relies on the integration of a notion of relaxed supports of linkage matching fields, an interpretation of the problem of bounded-rank matrix completion as a linear section problem on the Grassmannian, and a class of local coordinates on the Grassmannian described by Sturmfels and Zelevinsky in 1993.

Manolis Tsakiris
Chinese Academy of Sciences, China

manolis@amss.ac.cn

MS91

Algebraic Compressed Sensing

Compressed sensing deals with recovering a data-sparse vector from, usually, linear measurements. We introduce the broad subclass of algebraic compressed sensing problems, where the data-sparse, structured vectors are modeled either explicitly or implicitly via polynomials. This includes, for instance, low-rank matrix and tensor recovery. We employ powerful techniques from algebraic geometry to study well-posedness of sufficiently general compressed sensing problems, including existence, local recoverability, global uniqueness, and local smoothness. Our main results are summarized in thirteen questions and answers in algebraic compressed sensing. Most of our answers concerning the minimum number of required measurements for existence, recoverability, and uniqueness of algebraic compressed sensing problems are optimal and depend only on the dimension of the model.

Paul Breiding
University Osnabrück
Germany
pbreiding@uni-osnabrueck.de

Fulvio Gesmundo
University of Saarland
gesmundo@cs.uni-saarland.de

Mateusz Michalek
University of Konstanz
mateusz.michalek@uni-konstanz.de

Nick Vannieuwenhoven
Departement Computerwetenschappen
KU Leuven
nick.vannieuwenhoven@kuleuven.be

MS92

Formal Orientations of Isogeny Graphs

With Leonardo Col, we introduced the an orientated covering graph of the supersingular graph, obtained by imposing compatible embeddings of a CM field in the endomorphism algebra of each curve. In this work we consider the role of a formal orientation – equipping the formal group of each curve with compatible (formal) endomorphism rings.It is well known that the endomorphism ring is the p-adic completion of the endomorphism ring and every such formal group is isomorphic. We explore the implications for effective computation and navigation in the supersingular isogeny graph. This is joint work with Leonary Col.

David Kohel
Aix-Marseille Universite, France
david.kohel@univ-amu.fr

MS92

Hidden Stabilizers and the Isogeny to Endomorphism Ring Problem

We study the problem of computing the endomorphism ring of the codomain of a secret isogeny between supersingular curves in characteristic p given a representation for this isogeny, i.e. a way to evaluate this isogeny on any torsion point. This problem, that we call the Isogeny to Endomorphism Ring Problem (IsERP), plays a central role in isogeny-based cryptography and is at the heart of the recent attacks that broke the SIDH key exchange. However, no efficient algorithm is known to solve the IsERP for a generic degree, and the hardest case seems to be when the degree is prime. The key exchange pSIDH recently proposed by Leroux bases its security on the prime-degree version of the IsERP. We propose a quantum polynomial-time attack with subexponential classical precomputation (computation that only depends on the starting curve and the degree but not on the secret isogeny) on IsERP for any isogeny degree. A key implication of this is that one should not reuse the starting curve and the degree in pSIDH. We use two main tools: the group action of $(\mathrm{End}(E)/N\mathrm{End}(E))^*$ on the set of N-isogenies and a related non-abelian hidden subgroup problem that can be solved in quantum polynomial time.

Péter Kutas
Eötvös Loránd University
University of Birmingham
p.kutas@bham.ac.uk

Gábor Ivanyos
Institute for Computer Science and Control
Eötvös Loránd Research Network
gabor.ivanyos@sztaki.hu

Muhammad Imran
Budapest University of Technology and Economics
muh.imran716@gmail.com

Antonin Leroux
Inria and Laboratoire dInformatique de lEcole
polytechniqu
antonin.leroux@polytechnique.org

MS92

Deuring for the People: Supersingular Elliptic Curves with Prescribed Endomorphism Ring in General Characteristic

The *Deuring correspondence* relates maximal orders in certain quaternion algebras to supersingular elliptic curves, by identifying a quaternion order with the endomorphism ring of a curve. It is foundational to large swaths of contemporary isogeny-based cryptography, both as an attack tool and as a constructive building block. In this presentation, I will review the standard approach to computing the Deuring correspondence efficiently, and report on some recent algorithmic improvements and implementation results for general inputs. This line of work complements techniques known from the *SQISign* signature scheme, which makes heavy use of carefully selected, more favourable parameters.

Jonathan Komada Eriksen
Norwegian University of Science and Technology
jonathan.k.eriksen@ntnu.no

Lorenz Panny
Academia Sinica, Taipei, Taiwan
lorenz@yx7.cc

Jana Sotáková
University of Amsterdam
QuSoft
ja.sotakova@gmail.com

Mattia Veroni
Norwegian University of Science and Technology
mattia.veroni@ntnu.no

MS92

Setting the Stage: Isogeny-Based Cryptography

The cryptographic community is actively looking for alternatives for protecting our data and communications from adversaries with a large quantum computer. One of the most recent families of cryptosystems studied as part of this quest emerges from hard problems related to the isogeny graph of elliptic curves over finite fields. This minisymposium brings together presentations that focus on various aspects of isogenies and their applications in post-quantum cryptography. The topics that will be covered include cryptanalysis, protocol designs, and building secure implementations. The goal of this introductory talk is to present the mathematical background, give an overview of recent advances, and introduce the program.

Monika Trimoska
Radboud University
monika.trimoska@ru.nl

MS93

Fast Decoding of Ag Codes

In a recent paper by Beelen, Rosenkilde and Solomatov, fast linear algebra techniques and Hermite-Pade approximation was used to decode AG codes coming from algebraic curves very fast. More precisely, it was explained how for any AG code an instance of the famous Guruswami-Sudan list decoding algorithm can be performed faster than previously known. The main geometric ingredient in the description and complexity of these algorithms was the multiplicity of the Weierstrass semigroup of a suitably chosen point on the algebraic curve. In this talk, more subtle properties of the algebraic curve will be used to further improve the error-correcting capability of these fast decoding algorithms.

Peter Beelen
Technical University of Denmark
pabe@dtu.dk

Maria Montanucci
Department of Applied Mathematics and Computer Science
Technical University of Denmark
marimo@dtu.dk

MS93

Bounds and Constructions for Insertion and Deletion Codes

Insertion and deletion (insdel for short) codes have recently attracted a lot of attention due to their applications in many interesting fields such as DNA storage, DNA analysis, race track memory error correction and language processing. In this talk, we focus on bounds of insdel codes, such as insdel Singleton bound, upper bounds for code size, half-Singletion bound and bounds for alphabet size of Reed-Solomon codes.

Shu Liu
University of Electronic Science and Technology of Chia
shuliu@uestc.edu.cn

Chaoping Xing
Shanghai Jiao Tong University
xingcp@sjtu.edu.cn

MS93

Error Correction of Norm-Trace Codes Using Fewer Bits

The fractional decoding problem is motivated by the fact that in distributed systems there is usually a limitation on the disk operation as well as on the amount of information transmitted for the purpose of decoding. Sometimes thought of as error correction with partial information, fractional decoding considers codes defined over an extension field and algorithms for error correction that use fewer symbols from the base field than is typical, thus operating using a restricted amount of information in the decoding process. In this talk, we present two fractional decoding approaches for constant extension norm-trace codes. This research is joint work with Gretchen Matthews.

Welington Santos
Virginia Tech University
welington@vt.edu

Gretchen Matthews
Virginia Tech, U.S.
gmatthews@vt.edu

MS93

The Search for the Right Support: Better Bounds for the Lee Metric

One of the most important bounds in coding theory is the Singleton bound, which for the classical case of the Hamming metric is derived via a simple puncturing argument. Codes which attain the Hamming-metric Singleton bound are called Maximum Distance Separable (MDS) codes and it is well known that for large finite fields MDS codes are dense. This is fundamentally different to the current situation in the Lee metric, where the same puncturing argument leads to Shiromoto's bound. This bound, however, can only be achieved by one non-trivial linear code living in one ambient space. This implies that optimal codes with respect to Shiromoto's bound are sparse, whether we let the length of the code or the size of the underlying ring grow. The puncturing argument is thus not suitable for the Lee metric and an other technique is required. For this, we will turn to generalized weights. In order to define generalized Lee weights, we encounter several possibilities and discuss which definition of support will lead to good properties. This allows us to present a new Lee-metric Singleton bound, for which several optimal codes exist.

Violetta Weger
Technical University of Munich
violetta.weger@tum.de

Jessica Bariffi
German Aerospace Center
jessica.bariffi@dlr.de

MS94

Representability of the Direct Sum of q-Matroids

After a brief introduction of q-matroids, we will turn to their direct sum, which has been introduced in 2021 by Ceria/Jurrius. On the level of cryptomorphisms the theory of q-matroids forms a natural, yet non-trivial, q-analogue of matroid theory. However, this analogy stops when it comes to the direct sum. In this talk we will illustrate this discrepancy via representability. A q-matroid is called representable if it is induced by a vector rank-metric code. We will see that, different from matroids, the direct sum of representable q-matroids may not be representable. This is joint work with Benjamin Jany.

Heide Gluesing-Luerssen, Benjamin Jany
University of Kentucky
heide.gl@uky.edu, bja246@uky.edu

MS94

Q-Analogues of Applications of Matroids

Matroids are used in a variety of ways and have turned out to be a central tool in studying quite different topics. One such topic is error-correcting codes with the Hamming metric. Passing to Gabidulin rank-metric codes, it becomes clear that one should replace matroids by q-matroids. In this talk we ask whether q-versions of simplicial complexes and matroids, that is q-complexes and q-matroids, respectively, possibly could enter the picture also in other applications. We sketch how one can make Chow rings of q-matroids, and determine many of their properties, and we discuss q-versions of Delta-matroids, a tool designed for studying ribbon graphs on compact surfaces of positive genus. If time permits, we may also discuss Alexander duality of q-complexes.

Trygve Johnsen
University of Tromsø
trygve.johnsen@uit.no

MS94

Introduction to q-matroids and Related Structures

This talk aims to serve as an introduction to the minisymposium "q-Analogues in Combinatorics". A q-analogue in combinatorics can be seen as a generalization of the combinatorics of finite sets to that of finite dimensional vector spaces over the finite field GF(q). This session focusses on q-matroids, the q-analogue of matroids. We will discuss several cryptomorphic definitions of q-matroids. Some of these are a straightforward generalization of the similar definition for matroids; others are a highly non-trivial q-analogue. We argue, and this will be supported by later talks, that this is exemplary for q-analogues. The talk concludes with a short overview of what is coming next in this minisymposium.

Relinde Jurrius
Netherlands Defence Academy
rpmj.jurrius@mindef.nl

MS94

q-Matroids From q-partitions of Type t

In this talk, we introduce a q-analogue of the partitions of type-t, which appears as a generalization of subspace designs. Then, by following work by Byrne+, we consider q-matroid constructions from q-partitions of type t. This leads us to construct q-matroids which are not PMD from subspace designs. This is a joint work with Martin Bergamin.

Elif Saçikara
Aalto University
Finland
elif.sacikara@math.uzh.ch

MS95

Polynomials with Lorentzian Signature and Convexity

I will present the concept of polynomials with Lorentzian signature, which serves as a unifying framework for Lorentzian polynomials and hyperbolic polynomials. Furthermore, I will demonstrate that this class of polynomials satisfies the Hodge-Riemann (HR) relations for degrees up to 1. An interesting implication is to convert the problem of approximating the permanent of a special class of nonsingular matrices into the realm of hyperbolic programming. I shall illustrate the significant role of convexity to establish that the hyperbolicity cones, associated with the special class of nonsingular matrices coincide with the semipositive cones.

Papri Dey
Georgia Tech
pdey33@gatech.edu

MS95

Semidefinite Optimization Beyond Polynomials

Semidefinite programming relaxations have been very successfully used for nonconvex optimization problems involving polynomials. In this talk I will discuss how semidefinite optimization can be used for nonpolynomial problems. I will focus on applications in (quantum) information theory involving entropy functions.

Hamza Fawzi
Cambridge University
h.fawzi@damtp.cam.ac.uk

MS95

Smoothed Analysis of the Simplex Method

The simplex method is an important algorithm for finding points in convex polyhedra, when such a polyhedron is given in inequality description. Although this algorithm is very fast, we lack a theoretical understanding of why this is the case. In this talk I will describe some recent results about random convex polyhedra that come up when studying the simplex method.

Sophie Huiberts
Columbia University
sophie@huiberts.me

MS95

Introduction to Convexity

This talk is meant to serve as an introduction to the connections between convex geometry and algebraic geometry to those unfamiliar with the subject. We will try to touch on the topics which will be discussed by our speakers such as the combinatorial structure of polytopes, spectrahedra and their relations to algebra, and applications of convex geometry to algebraic geometry.

Kevin Shu
Georgia Institute of Technology

kshu8@gatech.edu

MS96

Absolute Concentration Robustness in Reversible Covalent Modification Networks With Arbitrary Deficiency

Shinar and Feinberg defined the notion of absolute concentration robustness (ACR) in reaction networks to mean that the concentration of a certain species (called ACR species) is invariant across all positive steady states. This means that even though the steady state values depend on initial concentrations, the ACR species concentration at steady state does not. Shinar and Feinberg gave a simple sufficient condition for existence of an ACR species, the network has a deficiency of one and two non-terminal complexes differ in the ACR species. The Shinar-Feinberg condition is not necessary and many biologically important networks do not have a deficiency of one. Previous experimental and modeling work had identified a bifunctional enzyme to be implicated in a mechanism for ACR in some reaction networks. We define bifunctionality in a large class of networks called reversible covalent modification networks, which includes n-site futile cycles or phosphorylation-dephosphorylation cycles. Such networks can have arbitrary deficiency. We give necessary and sufficient conditions for ACR in this class of networks.

Badal Joshi
California State University San Marcos
bjoshi@csusm.edu

Tung D. Nguyen
University of Wisconsin-Madison
daotung.nguyen@tamu.edu

MS96

A General Framework for Positive Solutions to Systems of Polynomial Inequalities with Real Exponents

We study positive solutions to parametrized systems of generalized polynomial *inequalitites* (with real exponents) in n variables and involving m monomial terms, that is, $x \in \mathbb{R}^n_>$ such that $(c \circ x^B) \in C$ with positive parameters $c \in \mathbb{R}^m_>$, exponents $B \in \mathbb{R}^{n \times m}$, convex ”coefficient” cone $C \subseteq \mathbb{R}^m_>$ (and component-wise product $\circ$). Our framework encompasses systems of generalized polynomial *equations*, as studied in real fewnomial and reaction network theory. We identify the relevant geometric objects of the problem, namely a bounded convex set P arising from the coefficient cone and two subspaces representing monomial differences and dependencies. The dimension of the latter subspace (the monomial dependency d) is crucial. As our main result, we rewrite the problem in terms of d monomial equations on the ”coefficient” set P, involving d monomials in the parameters. If $d = 0$, solutions exist (for all c) and can be parametrized explicitly, thereby generalizing monomial parametrizations (of ”toric” solutions). Even if $d > 0$, solutions on the coefficient set can be determined more easily than solutions of the original problem. Our theory allows a unified treatment of multivariate polynomial inequalities, based on linear algebra and convex geometry. We demonstrate its novelty and strength in applications to real fewnomial and reaction network theory.

Stefan Mueller
Faculty of Mathematics, University of Vienna
st.mueller@univie.ac.at

Georg Regensburger
Institute for Mathematics
University of Kassel
regensburger@mathematik.uni-kassel.de

MS96

Dimension of Steady State Varieties and Nondegenerate Equilibria

Understanding the dimension of the set of positive steady states of a network of interactions is a fundamental question. In particular, deciding conditions on a network which allow us to know whether each stoichiometric compatibility class has finitely many steady states for a generic choice or the reaction rates is useful for the application of known results in the field. For other applications, the existence of nondegenerate real positive steady states is a key property, and in fact these two features are related. I will present some results in this direction, based on joint work with E. Feliu and O. Henriksson.

Beatriz Pascual Escudero
Universidad Politécnica de Madrid
beatriz.pascual@upm.es

MS96

On Computing Polynomial Conservation Laws of Chemical Reaction Networks

We consider chemical reaction networks with mass-action kinetics, and discuss the problem of finding conservation laws of chemical reaction networks. Linear conservation laws are well-known, however, polynomial conservation laws are not fully investigated. We present algorithms for computing linear, monomial and polynomial conservation laws of chemical reaction networks, and for testing their completeness and independence. We discuss dependence of conservation laws on the parameters of a chemical reaction network and provide case distinctions on parameters, using comprehensive Grbner systems and parametric syzygies.

Hamid Rahkooy
University of Oxford
rahkooy@maths.ox.ac.uk

MS97

On the Marginal Independence Structure of DAG Models

We consider the problem of estimating the marginal independence structure of a DAG model from observational data. In order to so, we divide the space of directed acyclic graphs (DAGs) into certain equivalence classes, where each class can be represented by a unique undirected graph called the unconditional dependence graph. The unconditional dependence graphs satisfy certain graphical properties, namely having equal intersection and independence number. Using this observation, we can construct a Grobner basis for an associated toric ideal and define additional binomial relations to connect the space of unconditional dependence graphs. With these moves, we can implement a search algorithm, GrUES (Grobner-based Unconditional Equivalence Search), that estimates the conditional independence structure of the graphical model. The implementation shows that GrUES recovers the true marginal independence structure via a BIC-optimal or MAP estimate at a higher rate than simple independence tests while also yielding an estimate of the posterior. This is joint work with Alex Markham, Pratik Misra and Liam Solus.

Danai Deligeorgaki
KTH
danaide@kth.se

MS97

Directed Gaussian Graphical Models with Toric Vanishing Ideal

Directed Gaussian graphical models are statistical models that use a directed acyclic graph (DAG) to represent the conditional independence structures between a set of jointly random variables. The study of generators of the vanishing ideal of a DAG is an important problem for constraint based inference for inferring the structure of the underlying graph from data. In this talk, I will make an attempt to characterize the DAGs whose vanishing ideals are toric. In particular, I will give some combinatorial criteria to construct such DAGs from smaller DAGs which have toric vanishing ideals. In the end, for DAGs having toric vanishing ideal, I will present some results about the generating sets of those ideals.

Pratik Misra
KTH Royal Institute of Technology
pratikm@kth.se

MS97

Linear Causal Disentanglement

Causal disentanglement seeks a representation of data involving latent variables that relate to one another via a causal model. We consider linear causal disentanglement: observed variables that are a linear transformation of a linear latent causal model. The setup is identifiable if the linear transformation and the latent causal model are unique. We show that one intervention on each latent variable is sufficient and, in the worst case, necessary for identifiability. Based on joint work with Chandler Squires, Salil Bhate, and Caroline Uhler.

Chandler Squires
Massachusetts Institute of Technology
csquires@mit.edu

Anna Seigal
Harvard University, U.S.
aseigal@seas.harvard.edu

Salil Bhate
Broad Institute of MIT and Harvard
sbhate@broadinstitute.org

Caroline Uhler
Massachusetts Institute of Technology
cuhler@mit.edu

MS97

Introduction to Algebraic Methods in Graphical Models

In this talk we introduce graphical models from an algebraic perspective. A graph defines a multivariate statistical model where the nodes correspond to random variables and the edges encode relations between them. If the relations are linear, the covariances as well as higher order moments show interesting polynomial relations, especially if some of the nodes correspond to latent random variables. We discuss the example of factor analysis models that correspond to directed graphs, where edges only point from latent to observed nodes. In particular, we study the vanishing ideal of covariances when sparsity is introduced, that is, only a subset of the latent nodes have an edge pointing to an observed node.

Mathias Drton
Technische Universität München, Germany
mathias.drton@tum.de

Alexandros Grosdos, Irem Portakal
Technical University of Munich
alex.grosdos@tum.de, irem.portakal@tum.de

Nils Sturma
Technische Universität München
nils.sturma@tum.de

MS98

Tensor Decomposition for Compression of Convolution Layers in Deep Learning

Deep convolutional neural networks (CNNs) became the key tool in the field of computer vision with the advent of efficient computational tools notably graphical processing units (GPUs). One of the issues of the CNNs is the large number of weights (parameters) in the convolutional layers, the basic building blocks of the CNNs; thus an important question is how to reduce the computational and storage cost. In this talk, we propose a tensor approximation technique for compressing the underlying tensor of weights, also called kernel tensor (this kernel tensor is of order 3 and 4 for one- and two-dimensional convolution respectively). Our method is builds up on the approach pioneered by the work of [Lebedev et al, ICLR 2015], who proposed to use the CP decomposition (CPD) to compress the kernel tensor. The particular advantage of the CPD is that it decomposes the multidimensional convolution into simpler one-dimensional operations. We propose to use a novel regularization term and show how to develop an alternating least squares algorithm for optimizing the underlying cost function.

Rima Khouja
CRAN and IECL, France
rima.khouja@univ-lorraine.fr

MS98

Moment Estimation for Nonparametric Mixture Models Through Implicit Tensor Decomposition

TBA

Joe Kileel
University of Texas at Austin, U.S.
jkileel@math.utexas.edu

MS98

Quantum Max-Flow in the Bridge Graph

The quantum max-flow quantifies the maximal possible entanglement between two regions of a tensor network state for a fixed graph and fixed bond dimensions. In this talk, we calculate the quantum max-flow exactly in the case of the *bridge graph*. The result is achieved by drawing connections to the theory of prehomogenous tensor spaces and the representation theory of quivers.

Vincent Steffan
University of Copenhagen, Denmark
vincent.steffan@googlemail.com

MS99

Simultaneous Conjugation of Tuples of Matrices

Consider the action of GL(n) on m-tuples of $n \times n$ matrices.I will give an overview of the invariant theory related to this action and its connections to representation theory of algebras, algebraic complexity theory and operator theory. I will also discuss recent work with Igor Klep, Visu Makam and Jurij Volcic that gives a proof and a counterexample to two versions of a conjecture of Hadwin and Larson.

Harm Derksen
Northeastern University
Department of Mathematics
ha.derksen@northeastern.edu

Igor Klep
University of Ljubljana, Department of Mathematics
Slovenia
igor.klep@fmf.uni-lj.si

Visu Makam
University of Melbourne, Australia
visu.makam@unimelb.edu.au

Jurij Volcic
Drexel University
jurij.volcic@drexel.edu

MS99

Asymptotic Phenomena

The main topic of this series of mini-symposia is stability phenomena in various settings. One main question is whether a series of algebraic structures with maps between them can be characterized by a finite segment. In this introductory talk, I will share a few examples from algebraic statistics, commutative algebra, and algebraic geometry in which such a question arises (and answer that question in some cases). I will also say a few words about categories that provide a useful framework to approach these types of questions.

Rob Eggermont
Eindhoven University of Technology
R.H.Eggermont@tue.nl

MS99

Equivariant Hilbert Series, Segre Products and Regular Languages

A hierarchical model can be described by a toric ideal in a polynomial ring in variables indexed by the state space. In order to study simultaneously properties of these ideals for varying numbers of states equivariant Hilbert series have been considered. Using regular languages, it has been shown that these Hilbert series are rational functions in some cases. As a new tool, we introduce the Segre product of formal languages. By showing that the Segre product of two regular languages is again a regular language we establish rationality results in new cases.

Uwe Nagel
University of Kentucky
uwe.nagel@uky.edu

Aida Maraj
Max Planck Institute for Mathematics in the Sciences
maraja@umich.edu

Aida Maraj
University of Michigan
maraja@umich.edu

MS99

Symmetries and Local-global Principles in Discrete Geometry

We consider cones, monoids and related objects in infinite dimensional spaces which are invariant under actions of symmetric groups. A key idea is to study these objects via associated symmetric chains of cones, monoids, etc. in finite dimensional spaces and to formulate related local-global principles. In this talk we discuss recent results and open questions on these topics.

Tim Römer
Universität Osnabrück
troemer@uos.de

MS100

On Grbner Bases Over Dedekind Domains

Grbner bases are a fundamental tool when studying ideals in multivariate polynomial rings. More recently there has been a growing interest in transferring techniques from the field case to other coefficient rings, most notably Euclidean domains and principal ideal rings. In this paper we will consider multivariate polynomial rings over Dedekind domain. By generalizing methods from the theory of finitely generated projective modules, we show that it is possible to describe Grbner bases over Dedekind domains in a way similar to the case of principal ideal domains, both from a theoretical and algorithmic point of view.

Tommy Hofmann
University of Siegen, Germany
tommy.hofmann@uni-siegen.de

MS100

Algorithms for Determinantal Singularities

Beyond complete intersections and binomial ideals, determinantal ideals have attracted interest as a particular larger class of ideals which is still accessible to structured research. Their study has a long history in commutative algebra and algebraic geometry, but in the local (analytic) setting of singularity theory they have only moved into focus in recent years. This talk will outline two questions from the study of determinantal singularities and explain how an algorithmic approach relying on the determinantal property was the starting point for solving the respective tasks. (Joint work with Aline Bartel and Sabrina Gaube.)

Anne-Frühbis Krüger
Universität Oldenburg

anne.fruehbis-krueger@uol.de

MS100

Polynomial Systems Arising in Program Synthesis

Multiple classical problems in the formal verification of programs such as reachability, termination, and template-based synthesis can be reduced to solving polynomial systems of equations. In this talk, I will describe the primary objects and these connections. In particular, I will show how the algebraic and geometric techniques can be applied, enhancing the scalability and completeness for such problems.

Fatemeh Mohammadi
KU Leuven
fatemehmohammadi@kuleuven.be

MS100

Robust Parameter Estimation in ODE models

We present a new approach for parameter estimation in ODE models from measured data. Briefly, in a typical existing approach, the user tries to make a good initial guess for the parameter values. Then, in a loop, the corresponding outputs are computed by solving the ODE numerically, followed by computing the error with the given outputs. If the error is small, then the loop terminates and the parameter values are returned. Otherwise, heuristics/theories are used to possibly improve the guess and continue the loop. The main downside of this approach is non-robustness, as there are no guarantees for the convergence of loop iterations to true parameter values. Our new approach is robust. In particular, it does not require making good initial guesses for the parameter values. Instead, it uses differential algebra, interpolation of the data using rational functions, and multivariable polynomial system solving, and has a potential for a complete user control over the error of the estimation (the actual error analysis is left for the future research). This is joint work with Soo Go, Hoon Hong, Ilia Ilmer, Pedro Soto, and Chee Yap.

Alexey Ovchinnikov
CUNY Queens College and Graduate Center
aovchinnikov@qc.cuny.edu

MS101

Computational Problems in Probabilistic Reasoning

Conditional independence is used in statistics to describe information-theoretical ”special position” relations among jointly distributed random variables. Inferring conditional independence consequences from assumptions reduces to deciding whether a semialgebraic set is empty or not. In this talk we investigate the CI inference problem for four binary random variables which yields semialgebraic sets in 16-dimensional space with a particular combinatorial flavor. We employ a range of techniques and heuristics from SAT solving over polyhedral geometry to numerical and symbolic algebraic geometry. This talk is based on joint work with Ben Hollering and Tabea Bacher.

Tobias Boege
Aalto University
tobias.boege@aalto.fi

MS101

Algebraic Time-Reversible Models in Phylogenetics

To study the evolutionary history of a set of nucleotide sequences, one considers a Markov process on a phylogenetic tree specified by a nucleotide substitution model. This Markov process gives rise to the so-called phylogenetic variety of the tree, which can be used afterwards to desing phylogenetic reconstruction methods. For some simple nucleotide substitution models, a change of coordinates can be made to ease the study of these varieties. For example, for group-based models a discrete Fourier transform provides a monomial parametrization of the phylogenetic variety. Unfortunately, these models might be too simple to have real interest in biology. In this talk we will present a new algebraic approach that can handle a much larger family of substitution models: stationary and time-reversible models that are widely used in phylogenetics. We will see how these new tools allow the computation of equations that define the phylogenetic variety and generalize the tools used for group-based models.

Marta Casanellas
Departament de Matematiques
Universitat Politècnica de Catalunya
marta.casanellas@upc.edu

Jesus Fernandez Sanchez
Universitat Politechnica de Catalunya
jesus.fernandez.sanchez@upc.edu

Roser Homs Pons
Centre de Recerca Matemàtica, Spain
rhoms@crm.cat

Angelica Torres
Centre de Recerca Matemàtica
atorres@crm.cat

MS101

Symmetry Reduction in Am/gm Optimization

Besides sums of squares, alternative methods have been recently introduced to certify the non-negativity of polynomials. The arithmetic mean/geometric mean-inequality (AM/GM-inequality) facilitates classes of non-negativity certificates and of relaxation techniques for polynomials and, more generally, for exponential sums. We present a study of the AM/GM-based techniques in the presence of symmetries under the action of a finite group. This includes a symmetry-adapted representation theorem and techniques to reduce the size of the resulting relative entropy programs and speed-up numerical computations. In the case of the symmetric group, we can evaluate precisely this complexity gain and obtain certain stabilization results. As a consequence, we can exhibit several sequences of examples in growing dimensions where the size of the reduced problem stabilizes. Moreover, we will discuss more theoretical aspects such as the comparison between the associated cones and the cone of non-negative symmetric polynomials.

Philippe Moustrou
Institut de Mathématiques de Toulouse
Université Toulouse Jean Jaurès
philippe.moustrou@math.univ-toulouse.fr

Helen Naumann
J.W. Goethe University, Frankfurt am Main
naumann@math.uni-frankfurt.de

Cordian Riener
UiT The Arctic University of Norway
cordian.riener@uit.no

Thorsten Theobald
J.W. Goethe-Universität
Frankfurt am Main, Germany
theobald@math.uni-frankfurt.de

Hugues Verdure
UiT The Arctic University of Norway
hugues.verdure@uit.no

MS101

Welschinger Signs and the Wronski Map

A general real rational plane curve C of degree d has $3(d-2)$ flexes and $(d-1)(d-2)/2$ complex double points. Those double points lying in $\mathbb{R}P^2$ are either nodes or solitary points. The Welschinger sign of C is $(-1)^s$, where s is the number of solitary points. When all flexes of C are real, its parameterization comes from a point on the Grassmannian under the Wronskii map, and every parameterized curve with those flexes is real (this is the Mukhin-Tarasov-Varchenko Theorem). Thus to C we may associate the local degree of the Wronskii map, which is also ±1. My talk will discuss work with Brazelton towards a possible conjecture that that these two signs associated to C agree, and the challenges to gathering evidence for this.

Frank Sottile
Texas A&M University
sottile@tamu.edu

MS102

Constructing Integrands from Oriented Matroids: Locally Planar Generalized Biadjoint Scalar Amplitudes

In theoretical particle physics, the notion of planarity is a powerful tool; roughly, it restricts to the case of graphs embedded in a disk. The seminal work of Arkani-Hamed, Bourjaily, Cachazo, Goncharov, Postnikov and Trnka, relates the singularities of planar N=4 super Yang-Mills amplitudes to residues of a certain logarithmic differential form on G+(k,n), known as the Parke-Taylor factor. These residues are supported on positroid cells in the nonnegative Grassmannian. Parke-Taylor factors were used recently by Cachazo, Early, Guevara and Mizera (CEGM) in the scattering equations formula for (planar) generalized biadjoint scalar amplitudes. In this talk, we introduce the combinatorial calculus of Generalized Color Orders, to define locally planar CEGM amplitudes, one for each realizable oriented uniform matroid. We introduce an oriented analog of the Dressian and tropical Grassmannian; we conjecture an identity relating locally planar CEGM amplitudes to the corresponding chirotopal tropical Grassmannian. Based on joint work with Cachazo and Zhang.

Nick Early
MPI Leipzig
nick.early@mis.mpg.de

MS102

Cluster Symmetries and How To Compute Them

Cluster structures (e.g. cluster algebras, varieties, etc.) have recently found many applications within mathematics and physics. In particular, the cluster algebra structure underlying the coordinate ring of the Grassmannian Variety has proven to be important in the computation of scattering amplitudes in N=4 SYM theory and to the computation of polylogarithm relations. A key piece of data that a cluster structure encodes is its automorphism group or ”Cluster Modular Group”. This group is a generalisation of the mapping class group of a surface and provides surprising new symmetries of well studied objects such as the Grassmannian. In this talk I will give a brief introduction to the notion of a cluster structure, define the cluster modular group and show some explicit examples of its computation in the case of the Grassmannian.

Dani T. Kaufman
University of Copenhagen
dk@math.ku.dk

MS102

Adjoints of Amplituhedra

We will discuss the real algebraic geometry of amplituhedra in the special case that the amplituhedra are semialgebraic subsets of the Grassmannian of lines in projective 3-space. In particular, we will look at set partitions (aka triangulations in this context), algebraic boundaries, residual arrangements, and adjoint divisors. This is currently ongoing work with Simon Telen.

Rainer Sinn
University of Leipzig
rainer.sinn@uni-leipzig.de

MS103

Dimension Results for Polynomial Systems Over Complete Toric Varieties

A common computational approach to study affine varieties is to first homogenize the input defining equations. Among other reasons, we do so because the new equations have an associated grading that allows us to reduce our computations to a linear algebra problem. However, the homogenization process might introduce higher components at infinity, changing drastically the geometry of the affine object that we want to study. This is what happens when we homogenize, in the classical sense, sparse polynomials. To overcome this issue, a possible approach is to homogenize the input equations, using their Newton polytopes, over a Cox ring or a polytopal graded subring of it. However, other simpler homogenizations might be possible. In this work, we prove a combinatorial criterion to decide when a candidate homogenization is good, in the sense that it does not introduce higher components at infinity. Additionally, we use our criterion to decide which families of degrees on polytopal algebras lead to regular sequences.

Matías R. Bender
INRIA Saclay
CMAP, CNRS, École polytechnique, IPP
matias.bender@inria.fr

Pierre-Jean Spaenlehauer
INRIA
pierre-jean.spaenlehauer@inria.fr

MS103

Structured Polynomial Systems From Applications: Angles-only Orbit Determination and Radial Camera Relative Pose

I will describe two applications where parametric families of polynomial systems having special structure appear. In view of the theme of this minisymposium, I should point out that any explanation of this special structure using BKK or analogous root-counting technology is presently unavailable. Instead, the Galois/monodromy groups of these systems provide the essential clues. The first application (joint with Christian, Leykin, and Mancini) concerns orbit determination from line-of-sight measurements. The second application (joint with Hruby, Korotysnkiy, Oeding, Pollefeys, Pajdla, Larsson) comes from computer vision, and concerns estimating the relative orientation of radially-distorted pinhole cameras.

Timothy Duff
University of Washington
Seattle, WA
timduff@uw.edu

MS103

Kouchnirenko Formula and the Mixed Volume

Consider a collection of subpolytopes $P_1, \ldots, P_n$ of a n-dimensional polytope P. The inequality $MV(P_1, \ldots, P_n) \leq Vol(P)$ is implied by the monotonicity of the mixed volume. The equality occurs if and only if for each face $F \subsetneq P$ there are at least $dim(F)+1$ of polytopes intersecting it. The mixed volume decreases when reducing the bound to $dim(F)$ and we will give a combinatorial formula for the mixed volume $MV(P_1, \ldots, P_n)$ in this case under some restrictions on the polytopes $P_1, \ldots, P_n$. This formula is a part of a non-negative analogue of the Kouchnirenko formula for the Milnor number and is essential in proving that the analogue is indeed non-negative.

Fedor Selyanin
Skolkovo Institute of Science and Technology, Moscow, Russia
and National Research University Higher School of Economics
fed.se98@yandex.ru

MS103

Plcker-type Inequalities and Configuration Spaces of Mixed Volumes

Consider n plane convex bodies and compute their pairwise mixed areas. We show that starting with $n = 4$ these $\binom{n}{2}$ numbers satisfy certain quadratic inequalities similar to the Plcker relations for the Grassmannian. Moreover, for $n = 4$ they provide a complete description of all relations between the six mixed areas. This result is related to an old open problem (Heine 1938, Shephard 1960) of giving an algebraic inequality description for the space of all possible values of mixed volumes of n bodies in $\mathbb{R}^d$. I will talk about this connection as well as an application of our results to intersections of toric/tropical plane curves.

Ivan Soprunov
Cleveland State University
Department of Mathematics
i.soprunov@csuohio.edu

Gennadiy Averkov
BTU Cottbus - Senftenberg
Department of Algorithmic Mathematics
averkov@b-tu.de

MS104

Restriction and Extension for Planar Splines

If a planar triangulation is altered by adding a triangle in a shelling order, we study the corresponding effect on spline spaces. This leads to two exact sequences; one for restricting splines and another for extending splines. Using the restriction sequence we recover a result of Hong that the dimension of the planar spline space is given by Schumaker's lower bound for degrees at least 3r+2. Alfeld and Schumaker showed that Hong's bound can, in most cases, be reduced to 3r+1. From the extension sequence we indicate a hopeful path to (slightly) reduce the number 3r+1.

Michael R. DiPasquale
University of South Alabama
mdipasquale@southalabama.edu

MS104

An Algebraic Perspective to Splines

Splines are known as piecewise polynomial functions defined on polyhedral complexes that agree up to a smoothness degree at the intersection of faces. These functions arise in many areas of mathematics and industry, such as numerical analysis, approximation theory, topology, data interpolation, and computer-aided modeling. In 2015, Gilbert, Tymoczko, and Viel extended the concept of spline into an algebraic setting by introducing generalized splines. Given a finite graph G and a commutative ring R with identity, an edge labeling of G is a function α that assigns an ideal of R to each edge of G. The pair (G, α) is called an edge labeled graph. A generalized spline on (G, α) is a vertex labeling, such that the difference of labels on adjacent vertices lies in the corresponding edge label ideal. In this talk, we focus on generalized splines. We first discuss the motivation of the concept. Then, we compare generalized and classical splines, list the differences, and explain how these two settings of splines are related. Finally, we present some preliminary results on the algebraic structure of generalized splines.

Samet Sarioglan
Smith College
ssarioglan@hacettepe.edu.tr

MS105

Graph-Theoretic Algorithms for the Alternating Trilinear Form Equivalence Problem

At Eurocrypt‘22 Tang, Duong, Joux, Plantard, Qiao, and Susilo proposed a digital signature algorithm based on the hardness of the isomorphism problem of alternating trilinear forms. They propose three concrete parameters in dimensions 9, 10, and 11 respectively. We give new heuristic algorithms that solve this problem more efficiently. With our new algorithms, the first parameter set can be broken in less than a day on a laptop. For the second parameter set, we show there is a 2^{-17} fraction of the public keys that can also be broken in less than a day. We do not break the third parameter set in practice, but we claim it falls short of the target security level of 128 bits.

Ward Beullens
IBM Research
wbe@zurich.ibm.com

MS105

Practical Encryption Using Isogenies Between Elliptic Products

Recent attacks on SIDH have showed how to leverage torsion information to recover secret isogenies between elliptic curves. In this talk, we will explore how to use these techniques to obtain a trapdoor mechanism. Then, using standard transformations, we will derive a public-key encryption scheme, FESTA: Fast Encryption from Supersingular Torsion Attacks. The gist of this protocol is to combine 1-dimensional and 2-dimensional isogenies to achieve practical performance. This is joint work with Andrea Basso and Giacomo Pope.

Luciano Maino
University of Bristol
zu20014@bristol.ac.uk

MS105

SQISign Primes and How to Find Them

SQISign is a very promising post-quantum signature scheme, offering small signature and key sizes. For a fast performance, it requires a special prime characteristic in order for isogeny computations to be efficient. In particular, we require a large factor of $p^2 - 1$ to be smooth. In this talk, we discuss the exact requirements for SQISign-friendly primes, and different methods to find suitable parameters. E.g., this includes sieving techniques, and solving the related twin smooth integer problem.

Michael Meyer
University of Regensburg
michael@random-oracles.org

MS105

Superspecial Cryptography: Computing Isogenies Between Elliptic Products

Isogenies between abelian varieties stepped into the cryptographic spotlight in the Summer of 2022 when Kani's criterion guided cryptanalysts on a direct and efficient key recovery attack on the supersingular isogeny Diffie-Hellman (SIDH) problem. In a post-SIDH world, the cryptographic community is now considering constructive applications of higher dimensional isogenies for building new protocols. In this talk, we focus the implementation of $(2^k, 2^k)$-isogenies between superspecial abelian surfaces. These are precisely the isogenies used in the implemented attacks of SIDH as well as the recently proposed public key encryption protocol FESTA. We discuss implementation details and the current computational bottlenecks and compare costs to the more familiar dimension isogenies between elliptic curves.

Giacomo Pope
CryptoHacks
giacomopope@gmail.com

MS106

Involutions Over Finite Fields

In the context of memory-limited environments, involutions are desirable because they allow for efficient use of limited memory resources. Specifically, in many applications, both the permutation and its inverse must be stored in memory, which can be a challenge in resource-constrained environments. By using an involution as the interleaver, the same structure and technology used for encoding can be used for decoding as well. Fixed points are points that remain unchanged under the permutation. In cryptographic applications, such as the design of S-boxes, it is desirable to have permutations with a small number of fixed points to increase the security of the system. Therefore, understanding the number of fixed points and how to construct involutions with few fixed points is an important area of research. In this talk we will present some families of involutions over finite fields, including some explicit constructions based on a prescribed number of fixed points.

Ariane Masuda
NYCCT of CUNY
ariane.masuda70@citytech.cuny.edu

MS106

Which Numerical Sequences Are the Generalized Weights of a Code?

We characterize the numerical sequences which are the sequences of generalized weights of a linear block code, a rank-metric code, or a sum-rank metric code, over a field of large enough cardinality. The characterization is conditional on the existence of MDS, MRD, and MSRD codes, respectively.

Elisa Gorla
University of Neuchatel, Switzerland
elisa.gorla@unine.ch

Elisa Lorenzo Garcia, Umberto Martinez-Penas,
Flavio Salizzoni
University of Neuchatel
elisa.lorenzo@unine.ch, umberto.martinez@unine.ch,
flavio.salizzoni@unine.ch

MS106

Weierstrass Semigroups on a Maximal Curve With the Third Largest Genus

An $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$ of genus $g(\mathcal{X})$ is defined to be a projective, geometrically irreducible, non-singular algebraic curve defined over $\mathbb{F}_{q^2}$ such that the number of its $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil bound. Maximal curves, especially those with large genus, are of particular interest in coding theory since they give rise to excellent AG codes. It is well known that, for an $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$, it holds $g(\mathcal{X}) \leq \frac{q(q-1)}{2}$ and equality is reached if and only if $\mathcal{X}$ is $\mathbb{F}_{q^2}$-isomorphic to the Hermitian curve. Also the second largest genus of $\mathbb{F}_{q^2}$-maximal curves is known, as well as a characterization of the maximal curves attaining it, with respect to $\mathbb{F}_{q^2}$-isomorphism. Instead, the value of the third largest genus is known to be equal to $g_3 := \left\lfloor \frac{q^2-q+4}{6} \right\rfloor$, but finding a characterization of maximal curves with such a genus is a well-known open problem. In this talk, I will present our work concerning the Weierstrass semigroups on a curve which is known to have genus equal to g_3. One surprising result is that, unlike what happens for all the known maximal curves where the Weierstrass points are known, the set of Weierstrass points of this curve is much richer than the set of its $\mathbb{F}_{q^2}$-rational points.

Peter Beelen
Technical University of Denmark
pabe@dtu.dk

Maria Montanucci
Department of Applied Mathematics and Computer Science
Technical University of Denmark
marimo@dtu.dk

Lara Vicino
Technical University of Denmark
lavi@dtu.dk

MS106

On Classifying Linear Sets

It is known that every linear set can be obtained as a projection of a canonical subgeometry [G. Lunardon, O. Polverino, Translation ovoids of orthogonal polar spaces, Forum Math. 16 (2004) 663-669]. In [B. Csajbk, C. Zanella, On scattered linear sets of pseudoregulus type in $\mathrm{PG}(1, q^t)$, Finite Fields Appl. 41 (2016), 34-54; C. Zanella, F. Zullo, Vertex properties of maximum scattered linear sets of $\mathrm{PG}(1, q^n)$, Discrete Math. 343 (2020)] it was described how the properties of the vertex of such a projection are reflected in those of a linear set, especially with regard to linear sets contained in $\mathrm{PG}(1, q^n)$. For $n \leq 4$, this leads to a complete classification [G. Bonoli, O. Polverino, $\mathbb{F}_q$-linear blocking sets in $\mathrm{PG}(2, q^4)$, Innov. Incidence Geom. 2 (2005); B. Csajbk, C. Zanella, Maximum scattered $\mathbb{F}_q$-linear sets of $\mathrm{PG}(1, q^4)$, Discrete Mathematics 341 (2018), 74-80]. In this talk I will describe a classification also for $n = 5$, once again obtained by studying the vertex of the projection. Some of the classes found might in fact be empty. The work continues a research started in [M. Montanucci, C. Zanella, A class of linear sets in $\mathrm{PG}(1, q^5)$, Finite Fields Appl. 78 (2022) 101983]. Joint work with Giovanni Longobardi

Corrado Zanella
University of Padova
corrado.zanella@unipd.it

MS107

On the Theory of Blocks for Rank Metric Codes

In 1966, W.T. Tutte introduced the notion of blocks to approach the Critical Problem for binary matroids. In general, a *k-block over $GF(q)$* is a matroid with critical exponent strictly greater than k over $GF(q)$. A k-block M is called *minimal* if every proper restriction of M has critical exponent less than or equal to k. Thus, solving the Critical Problem is equivalent to classifying such blocks. In this talk, we extend the notion of blocks for matroids to (q, m)-polymatroids representable as Delsarte rank-metric codes, and then provide some examples and constructions of our q-analogue of blocks.

Koji Imamura, Keishuke Shiromoto
Kumamoto University
Japan
211d9321@st.kumamoto-u.ac.jp, keisuke@kumamoto-u.ac.jp

MS107

Maximum Sum-Rank Distance Codes Over Finite Chain Rings

In this talk, we will introduce maximum sum-rank distance (MSRD) codes and linearized Reed-Solomon codes over finite chain rings. We will provide several sec tensions of Lam and Leroy's results on the roots of skew polynomials to finite chain rings. Using them, we will show that linearized Reed-Solomon codes are MSRD and we will give a new quadratic-time syndrome decoder for them, which improves on the cubic-time Welch-Berlekamp decoder that we presented previously in WCC 2022. This work was done in collaboration with Sven Puchinger.

Umberto Martinez-Penas
University of Valladolid
Spain
umberto.martinez@uva.es

Sven Puchinger
Technical University of Denmark
sven.puchinger@tum.de

MS107

Linear Sets and the q-analogue of the Vosper Theorem for Finite Fields

Linear sets have been shown to be a powerful tool in several classification results and constructions of objects in finite geometry and coding theory, such as semifields, blocking sets, translation ovoids, KM-arcs, rank metric codes, etc.. The main topic of this talk regards special classes of linear sets on the projective line: the *minimum size linear sets* and the so called *clubs*. In [V. Napolitano, O. Polverino, P. Santonastaso, F. Zullo: Classifications and constructions of minimum size linear sets, arXiv:2201.02003] and [V. Napolitano, O. Polverino, P. Santonastaso, F. Zullo: Clubs and their applications, arXiv:2209.13339] we study such families providing classifications results and new constructions. One of the tools used to get such classification results is a generalization (under certain assumptions) of the linear analogue of the Vosper theorem for finite fields (see [C. Bachoc, O. Serra, G. Zmor: An analogue of Vosper's theorem for extension fields, *Math. Proc. Camb. Philos. Soc.* 163(3) (2017), 423-452.]). In this talk, after recalling some general results on linear sets on the projective line, we will give an overview of our results.

Vito Napolitano
University of Campania
vito.napolitano@unicampania.it

Olga Polverino
University of Campania Luigi Vanvitelli
Italy
olga.polverino@unicampania.it

Paolo Santonastaso
University of Caserta
paolo.santonastaso@unicampania.it

Ferdinando Zullo

Università degli Studi della Campania
ferdinando.zullo@unicampania.it

MS107

Critical Problem for Rank-Metric Codes

The *Critical Problem* (Crapo and Rota, 1970) in matroid theory is the problem of finding the maximum dimension of a subspace which does not intersect a fixed subset in a vector space over a finite field, or in the original statement of the problem, of finding the least number of hyperplanes whose intersection contains no element of the subset (cf. [J.P.S. Kung, Critical problems, in: Matroid Theory, Seattle, WA, 1995]). This least number was introduced in the context of matroid theory where it has attracted attention as the *critical exponent* of a representable matroid over a finite field. The *Critical Theorem*, which provides another approach to the Critical Problem, has been interpreted in terms of coding theory. In this talk, to formulate the Critical Problem for a q-analogue of polymatroids, we define the critical exponent of (q, m)-polymatroids from the characteristic polynomials as an analogue of that of representable matroids. We associate (q, m)-polymatroids with *Delsarte rank-metric codes* via a (q, m)-polymatroid analogue of the Critical Theorem.

Keishuke Shiromoto, Koji Imamura
Kumamoto University
Japan
keisuke@kumamoto-u.ac.jp, 211d9321@st.kumamoto-u.ac.jp

MS108

Gram Spectrahedra of Symmetric Binary Forms

I will report on the geometric and combinatorial structure of symmetry adapted Gram spectrahedra of symmetric binary forms. In particular, I will present a characterization of extreme points of these spectrahedra that are of rank two. This is complementary to a classical result in the non-symmetric case. I will also report what we know about the facial structure and combinatorics of the same spectrahedra.

Serkan Hosten
Department of Mathematics
San Francisco State University
serkan@sfsu.edu

MS108

Convex Cones and Their Properties: a Convex Geometry Perspective

There are many properties of facial structure of convex sets that coincide in a lower-dimensional setting but differ in higher dimensions. This talk will cover several such different properties and their relations, including facial exposure, facial dual completeness (niceness), amenability and projectional exposure. Even though the definitions of these properties have a different nature, they form a neat hierarchy. Based on an example of sufficient and necessary conditions for niceness obtained using lexicographic tangents, an argument can be made about a possibility to explain these different notions and their relations using a unified approach.

Vera Roshchina
School of Mathematics and Statistics
UNSW Sydney
v.roshchina@unsw.edu.au

MS108

Gale Diagrams for the PSD Cone

Studying the facial structure of polyhedra has been a vital part of research both from a combinatorial perspective as well as in optimization through linear programming. One tool developed for understanding the facial structure of polytopes is the Gale diagram. In joint work with Venkat Chandrasekaran and Amy Wiebe, we generalize this to a larger family of convex objects, spectratopes, linear images of the spectraplex. The spectraplex is the analogue of the simplex in the cone of positive semidefinite matrices, the cone of interest in semidefinite programming. We show that our Gale diagrams can be used to understand the facial structure of these new convex bodies.

Isabelle Shankar
Portland State University
Department of Mathematics and Statistics
isabelle.shankar@pdx.edu

MS108

The Diameter-Width-Ratio for Complete and Pseudo-Complete Sets

Complete sets in general Minkowski spaces are convex sets with the property that adding any additional point to the set enlarges its diameter. This property holds for all constant width bodies, and thus constant width always implies completeness, while the opposite is in general not true. Pseudo-complete sets are convex sets, for which the diameter is equal to the sum of the in- and circumradius. Moreover, pseudo-completeness implies completeness. We present results on the diameter-width-ratio for complete and pseudo-complete sets, depending on the Minkowski asymmetry measures of the convex body, which itself is bounded by the dimension of the ambient space.

Katherina von Dichter
TU Munich
dichter@ma.tum.de

MS109

Gramian Constructions of Sum-of-Squares Lower Bounds and the Spectra of Pseudomoments

I will present an approach to proving lower bounds in the sum-of-squares hierarchy of semidefinite programs that, unlike previous approaches, constructs pseudomoment matrices directly as Gram matrices of suitable collections of vectors. This allows many difficulties in proving positivity of pseudomoment matrices to be circumvented, and brings to light algebraic and combinatorial identities thanks to which pseudomoment matrices can simultaneously satisfy both the entrywise and the spectral constraints placed on them. The main example I will explore is the lower bound showing that low-degree sum-of-squares does not exactly represent the cut polytope, due independently to Grigoriev (2001) and Laurent (2003). I will show an alternative proof of this result using the "Gramian" construction of the underlying pseudomoments, as well as proofs of several empirical observations of Laurent's about the spectrum of those pseudomoments. I will also present the connection between this construction and the elegant geometry of homogeneous polynomials under the "apolar" inner product. Finally, time permitting, I will discuss the extension of these ideas to lower bounds for optimization problems over random inputs, focusing on the case of the Sherrington-Kirkpatrick Hamiltonian of statistical physics. Based partly on joint work with Cristopher Moore and Afonso Bandeira.

Dmitriy Kunisky
Yale University
dmitriy.kunisky@yale.edu

MS109
Convergence Rates for Sums-of-Squares Hierarchies in the Correlative Sparsity Case

Sum-of-squares schemes for polynomial optimization are celebrated for their ability to find certificates for global minima of semialgebraic optimization problems. A downside is the sometimes high complexity of the method when scaling the number of variables. To cope with this, a few algorithms have been proposed that leverage sparsity properties of polynomials. We present work that derives upper bounds on the convergence rate of the moment-sum-of-squares hierarchy with correlative sparsity. The main conclusion is that both sparse hierarchies based on the Schmdgen and Putinar Positivstellenstze enjoy a polynomial rate of convergence that depend on the size of the largest clique in the sparsity graph but not on the ambient dimension. Interestingly, the sparse bounds outperform the best currently existing bounds for the dense hierarchy when the maximum clique size is sufficiently small compared to the ambient dimension and the performance is measured by the running time of an interior point method required to obtain a bound on the global optimum of a given accuracy. Joint work with Milan Korda and Victor Magron.

Rodolfo Rios-Zertuche
LAAS-CNRS / ANITI
rodolforiosz@gmail.com

MS109
Degree Bounds for Putinar's Positivstellensatz on the Hypercube

The Positivstellenstze of Putinar and Schmdgen show that any polynomial f positive on a compact semialgebraic set can be represented using sums of squares. Recently, there has been large interest in proving effective versions of these results, namely to show bounds on the required degree of the sums of squares in such representations. These *effective* Positivstellenstze have direct implications for the convergence rate of the celebrated moment-SOS hierarchy in polynomial optimization. In this talk, we restrict to the fundamental case of the hypercube $\mathbb{B}^n = [-1,1]^n$. We show an upper degree bound for Putinar-type representations on $\mathbb{B}^n$ of the order $O(f_{\max}/f_{\min})$, where $f_{\max}$, $f_{\min}$ are the maximum and minimum of f on $\mathbb{B}^n$, respectively. Previously, specialized results of this kind were available only for Schmdgen-type representations and not for Putinar-type ones. Complementing this upper degree bound, we show a lower degree bound in $\Omega(\sqrt[8]{f_{\max}/f_{\min}})$. This is the first lower bound for Putinar-type representations on a semialgebraic set with nonempty interior described by a standard set of inequalities.

Lorenzo Baldi
Sorbonne Université, CNRS
PolSys - Polynomial Systems LIP6, Paris, France
lorenzo.baldi@inria.fr

Lucas Slot
ETH Zurich
lucas.slot@inf.ethz.ch

MS109
Complexity Results About the Exactness of Sum-of-Squares Approximations for Polynomial Optimization

We study polynomial optimization problems for which the Lasserre sum-of-squares hierarchy has finite convergence. Nie (2014) shows that if the problem has finitely many minimizers and they satisfy the classical optimality conditions, then finite convergence holds. Using this, he shows that finite convergence holds generically. In this talk we show that 1) testing whether a standard quadratic program has finitely many minimizers is NP-hard. Moreover, 2) testing whether the Lasserre hierarchy of a polynomial optimization has finite convergence is NP-hard. We finish with a discussion on new methods for showing finite convergence in the presence of infinitely many minimizers.

Luis Felipe Vargas
CWI
luis.vargas@cwi.nl

Monique Laurent
Centrum Wiskunde & Informatica (CWI)
Amsterdam, and Tilburg University
M.Laurent@cwi.nl

Markus Schweighofer
Universität Konstanz
markus.schweighofer@uni-konstanz.de

MS110
Some Algebraic Questions Arising from the Study of Bifurcations in Chemical Reaction Networks

Deciding whether a given chemical reaction network admits some bifurcation can often be reduced to a problem in algebra. Frequently, necessary conditions for bifurcation can be formulated in terms of the feasibility of some system of polynomial equations and inequalities derived from the network. Writing down a hierarchy of such necessary conditions for bifurcation (from simple to more complicated), and automating the process of checking these conditions, can rapidly give candidates for particular bifurcations. Further algebraic computations, often more challenging, can then be used to confirm the occurrence of bifurcations and characterise the bifurcation set. I will describe how this process has led to the classification of small mass action networks according to whether they admit particular bifurcations or not.

Murad Banaji
University of Oxford
murad.banaji@maths.ox.ac.uk

MS110
Computing the Focal Values of Andronov-Hopf Bifurcations in Mass-Action Systems

Probably the most powerful way to prove the existence of oscillations in mass-action systems is via Andronov-Hopf bifurcations. Checking the transversality of the bifurcation is usually rather easy, however, deciding whether it is nondegenerate is computationally challenging. The nondegeneracy can be answered by computing the first focal value (preferably symbolically, not only numerically): if it is negative (resp., positive), the bifurcation is supercritical (resp., subcritical), leading to a stable (resp., unstable) limit cycle. The source of the difficulties is a combination of multiple facts, including the high number of species, the presence of conservation laws, and the potentially complicated Routh-Hurwitz surface in parameter space. We present a class of three-species bimolecular mass-action systems, where we could compute and analyse the first focal value, thereby providing a classification of these systems according to the stability of the limit cycle that is born via an Andronov-Hopf bifurcation.

Balázs Boros
University of Vienna
borosbalazs84@gmail.com

MS110

Identifying Parameter Values for Oscillations in a Class of Reaction Networks

We present a method for identifying Hopf bifurcation points in ordinary differential equations (ODE) models with parameters for reaction network with n species. The method is based on a Hopf bifurcation theorem for parametric systems, algebraic geometry, majorization theory and convex analysis. The main difficulty related to identifying Hopf bifurcation points, lies with selecting parameter values such that the next to last Hurwitz determinant $\det H_{n-1}$ is zero. The usual process requires performing an extensive numerical search among all of the exponents of the Newton polytope of $\det H_{n-1}$ to find a vertex associated with a negative monomial. The existence of such a vertex usually guarantees finding parameter values such that $\det H_{n-1}$ is zero. We show that a vertex of the Newton polytope of $\det H_{n-1}$ exists among the exponents of the product of diagonal entries of H_{n-1} which significantly reduces the computational effort. If such a vertex is associated with a negative monomial, then finding candidates for Hopf bifurcation points becomes an easy enough problem. The method is applied to several examples of biochemical networks such as a glycolytic reaction, Ca^{++} ions reaction and a simplified MAPK network.

Maya Mincheva
Northern Illinois University
mmincheva@niu.edu

MS110

Multistationarity of Small Zero-One Networks

Zero-one networks are very common in cell signaling. In this talk, we will present the recent progress on the multistationarity problem of small zero-one networks. First, we show that if a zero-one network admits multistationarity, then the rank is at least three. Also, we show that the smallest multistationary zero-one network is rank-three, and it has three species and five reactions. Second, we classify all rank-one and rank-two zero-one networks according to if they admit one (stable) steady state or not.

Xiaoxian Tang
Beihang University, China
xiaoxiantang@icloud.com

MS111

Decomposable Context-Specific Models

In this talk I will introduce a family of discrete context-specific models that we call decomposable CSmodels. Then I will show that these models have many algebraic and combinatorial properties that generalize those of decomposable graphical models. These models are defined as a subclass of staged tree models and can be alternatively represented by a collection of context DAGs. This is joint work with Yulia Alexandr, Julian Vill based on previous work with Liam Solus.

Eliana Duarte
Centro de Matematica Universidade do Porto
Max-Planck-Institute for Mathematics in the Scinces
eliana.gelvez@fc.up.pt

Julian Vill
OvGU Magdeburg
julian.vill@ovgu.de

Yulia Alexandr
UC Berkeley
yalexandr@berkeley.edu

MS111

Huesler-Reiss Extremal Graphical Models

Extreme value theory aims to explain statistical phenomena whose occurrence probability is very low, such as extreme weather phenomena or financial crises. Extremal graphical models are an exciting and rapidly growing new direction in graphical modeling that allow the study of extremes in higher dimensions. In this talk we shed light on the algebraic structures of the Hsler-Reiss distributions underlying these models. We establish the connection between the Gaussian ideal of an undirected model and the corresponding extremal counterpart. Moreover we study the maximum likelihood degree for these models and contrast with the Gaussian case. We furthermore use colored graphical models in this setting and illustrate our results using real-world data. This is based on joint work with Frank Rttger and Jane Coons.

Jane Coons
St John's College, University of Oxford
jane.coons@sjc.ox.ac.uk

Alexandros Grosdos
Technical University of Munich
alex.grosdos@tum.de

Frank Röttger
Université de Genève
frank.roettger@unige.ch

MS111

Convex Covariance Matrix Estimation and Sparsity

In covariance matrix estimation often the challenge is to find a suitable model and an efficient method of estimation. Two popular approaches are to impose linear restrictions on the covariance matrix or on its inverse but linear restrictions on the matrix logarithm of the covariance matrix have been also considered. In this talk I will present a general framework for linear restrictions on various transformations of the covariance matrix. This includes the three examples mentioned above. The proposed estimation method relies on solving a convex problem and leads to an estimator that is asymptotically equivalent to the maximum likelihood estimator of the covariance matrix under the Gaussian assumption. After developing a general theory, we restrict our attention to the case where the linear constraints require certain off-diagonal entries to be zero. Here the geometric picture closely parallels what we know for the Gaussian graphical models.

Piotr Zwiernik
University of Toronto
piotr.zwiernik@utoronto.ca

MS112

Well-order for Equivalence Classes of Cubic Forms of Infinite Strength

Asymptotic algebraic geometry aims at highlighting structure and uniform behaviour up to the action of a symmetry group for geometric objects whose dimension tends to infinity. In most cases, the stabilisation behaviour can be guessed from big-enough finite dimensional instances. In this talk, we show that this is not always the case, and illustrate how cubic polynomials in any finite number of variables do not exhibit much structure relating them, while their infinite dimensional counterparts (infinite-strength cubic forms) are well-ordered up to the equivalence relation of a natural monoid acting on them. Conjecturally, this story continues for higher degree-d forms, whose equivalence classes might satisfy the descending chains condition. Keywords: strength of tensors, tensor spaces, isogeny classes, and residual rank. Joint work with Arthur Bik, and Andrew Snowden.

Alessandro Danelon
Eindhoven University of Technology
alessandro.danelon@unibe.ch

Arthur Bik
Institute for Advanced Studies
mabik@ias.edu

Andrew Snowden
University of Michigan
asnowden@umich.edu

MS112

A Gap in the Subrank of Tensors

Tensor subrank is a measure of how much a tensor can be “diagonalized” by applying linear maps on its tensor factors. In a sense, this is a notion dual to the classical tensor rank. Motivated by applications to extreme combinatorics, algebraic complexity and quantum information, one is interested in the growth of subrank under Kronecker powers of tensors. In recent work with Christandl and Zuiddam, we showed that either the subrank of all powers is 1 or its growth is exponential with a rate $c_k > 1$, depending only on the order of the tensor. In this talk, I will briefly explain the geometric ideas behind this result, and some possible generalizations.

Fulvio Gesmundo
University of Saarland
gesmundo@cs.uni-saarland.de

MS112

Topological Noetherianity of Infinite Spin Representations

In this talk we consider the infinite Spin group $Spin$, defined as the union of $Spin(2n)$ as n grows, and the geometry of its representations. Our main result states that the infinite half Spin representation is topologically $Spin$-Noetherian. As a consequence, similar to Draisma-Eggermonts work on Plcker varieties, we obtain that $Spin$-stable subvarieties of this representation are defined by the pullback of equations at a finite level. The main example for such subvarieties is the infinite isotropic Grassmannian in its Spinor embedding, for which we explicitly determine its defining equations following the analogous result in the case of the Plcker embedding as established by Seynnaeve-T. This talk is based on joint work with Christopher Chiu, Jan Draisma, Rob Eggermont and Tim Seynnaeve.

Nafie Tairi
Universität Bern
nafie.tairi@unibe.ch

Christopher Chiu
Eindhoven University of Technology
c.h.chiu@tue.nl

Jan Draisma
Mathematical Institute, University of Bern, Switzerland
jan.draisma@math.unibe.ch

Rob Eggermont
Eindhoven University of Technology
R.H.Eggermont@tue.nl

Tim Seynnaeve
KU Leuven
tim.seynnaeve@kuleuven.be

MS112

The Generic Subrank of Tensors

The subrank of a tensor measures how much the tensor can be diagonalised. This notion was introduced by Strassen in 1987 to study matrix multiplication algorithms, and is related to several problems in combinatorics and quantum information. We determine the subrank of random tensors (generic subrank), establishing a large gap between the subrank on the one hand and the slice rank, analytic rank and geometric rank on the other hand. This is joint work with Derksen and Makam.

Harm Derksen
Northeastern University
Department of Mathematics
ha.derksen@northeastern.edu

Visu Makam
University of Melbourne, Australia
visu.makam@unimelb.edu.au

Jeroen Zuiddam
University of Amsterdam.
j.zuiddam@uva.nl

MS113

Computing Riemann-Roch Spaces for Algebraic Geometry Codes

Reed-Solomon codes are a well-known technique to represent data in the form of vectors, such that the data can be recovered even if some vector coordinates are corrupted. These codes have many properties, e.g. they have optimal parameters and are compatible with the addition and multiplication of data. Nevertheless, they suffer from some limitations. For instance, the storage size of vector coordinates grows logarithmically with the number of coordinates. Algebraic Geometry (AG) codes are a generalization of Reed-Solomon codes that enjoys similar properties while being free of these limitations. Thus, the use of AG codes provides complexity gains and turns out to be useful in several applications such as distributed storage and zero-knowledge proofs. Algebraic Geometry codes are constructed by evaluating spaces of functions, called Riemann-Roch spaces, at the rational points on a curve. It follows that the computation of these spaces is crucial for the implementation of AG codes. In this talk, I will present a joint work with S. Abelard, A. Couvreur, and G. Lecerf on the effective computation of bases of Riemann-Roch spaces of curves. I will discuss the ideas behind our algorithm, including in particular Brill-Noether theory. The curves used in the construction of AG codes were for the most part limited to those for which the Riemann-Roch bases were already known. This new work and the ones that will follow will allow the construction of AG codes from more general curves.

Elena Berardini
CNRS, Université de Bordeaux
elena.berardini@math.u-bordeaux.fr

MS113

OSCAR – A new Computer Algebra System

The OSCAR project develops a comprehensive Open Source Computer Algebra Research system for computations in algebra, geometry, and number theory, with particular emphasis on supporting complex computations which require a high level of integration of tools from different mathematical areas. The project builds on and extends the four cornerstone systems GAP, Singular, polymake, and Antic, as well as further libraries and packages, which are combined using the Julia language. Though still under development, OSCAR is already usable. In this talk, I will give examples of what is possible right now, and outline future lines of development.

Wolfram Decker
TU Kaiserslautern
decker@mathematik.uni-kl.de

MS113

Multivariate Cryptography and the Complexity of Solving a Random Polynomial System

A multivariate cryptographic instance in practice is a multivariate polynomial system. So the security of a protocol relies on the complexity of solving a multivariate polynomial system. During this talk I will explain the invariant to which this complexity depends on: the solving degree. Unfortunately this invariant is hard to compute. We will talk about another invariant, the degree of regularity, that under certain condition, give us an upper bound on the solving degree. Finally we will talk about random polynomial systems and in particular what ”random” means to us. We will give an upper bound on both the degree of regularity and the solving degree of such random systems.

Giulia Gaggero
Université de Neuchatel
giulia.gaggero@unine.ch

MS113

Characteristic Decomposition: Connecting Lexicographic Groebner Bases and Triangular Sets

Lexicographic Groebner bases and triangular sets are standard computational tools for handling multivariate polynomial ideals. In this talk, I will first present new results on the intrinsic structures of lexicographic Groebner bases and the relations between lexicographic Groebner bases and the minimal triangular sets contained in them called W-characteristic sets. Then I introduce the concept of characteristic pair consisting of a reduced lexicographic Groebner basis and its W-characteristic set. The decomposition from any polynomial set into finitely many characteristic pairs with associated ideal and zero relations is called characteristic decomposition, and it provides representations of the ideal generated by the polynomial set in terms of Groebner bases and triangular sets simultaneously. Basic properties of the decomposition and the resulting characteristic pairs, in particular the relationships between the Groebner basis and W-characteristic set in each pair, will also be presented. This talk is based on the joint work with Dongming Wang and Rina Dong.

Chenqi Mou
Beihang University, China
chenqi.mou@buaa.edu.cn

MS114

Positivity Certificates for P-recursive Sequences

We consider real sequences that satisfy a linear recurrence relation with polynomial coefficients. Algorithms proving the positivity of such sequences are known for recurrences of order 2 or for recurrences of arbitrary order with constant coefficients and whose characteristic polynomial admits a single dominant root. We design an algorithm to prove the positivity for recurrences with polynomial coefficients of arbitrary order, under the same condition on the characteristic polynomial. This algorithm is illustrated by several sequences from the literature.

Alaa Ibrahim, Alaa Ibrahim
ENS de Lyon
France
alaa.ibrahim@inria.fr, alaa.ibrahim@inria.fr

MS114

Certificates of Non-Negativity on Semi-Algebraic Subsets of Cylinders

A certificate of non-negativity (resp. positivity) for a polynomial $f \in \mathbb{R}[\mathbf{x}] = \mathbb{R}[x_1, \ldots, x_n]$ on a semialgebraic set $S \subset \mathbb{R}^n$ is an algebraic identity that makes evident the fact that $f(x) \geq 0$ (resp. $f(x) > 0$) for every $x \in S$. These certificates go back to the classical Positivstellenstaz proved by Krivine in 1964, and they have been widely studied and applied since then. In this talk, we will present a Putinar-Vasilescu like certificate of non-negativity for a polynomial f that is positive on a non-compact semialgebraic set $S = \{x \in \mathbb{R}^n \mid g_1(x) \geq 0, \ldots, g_s(x) \geq 0\}$ included in a cylinder. Under certain assumptions on f and the polynomials $g_1, \ldots, g_s \in \mathbb{R}[\mathbf{x}]$ defining S, we will show the existence of the proposed certificate of non-negativity of f and explain how one can obtain an upper bound for the degrees of the polynomials appearing in the representation.

Gabriela Jeronimo
Universidad de Buenos Aires and Conicet, Argentina
jeronimo@dm.uba.ar

Daniel Perrucci
Departamento de Matemática
Universidad de Buenos Aires
perrucci@dm.uba.ar

MS114

Convex Hulls of Space Parametric Curves: An Exact Computation Approach

We present an algorithm and its bit-complexity for computing the convex hull of space parametric curves. The boundary of the convex hull is a semi-algebraic set and an exact representation, breaks it down to a set of triangles and developable surface patches. We show that its computation reduces to isolating roots of a univariate polynomial with coefficients in a (multiple) extension field. We obtain bit-complexity results for the latter operation using amortized bounds on the roots of the polynomial.

Christina Katsamaki
Inria Paris & IMJ-PRJ
Sorbonne Université
christina.katsamaki@inria.fr

Fabrice Rouillier
INRIA
Fabrice.Rouillier@inria.fr

Elias Tsigaridas
Inria Paris
elias.tsigaridas@inria.fr

MS114

Diophantine Obstructions and Probabilistic Speed-Ups for Discriminants

A fundamental problem underlying real root counting, and the determination of isotopy types of real zero sets, is querying the side of a discriminant variety on which one lies. We show how this problem relates to other (nearly) NP-hard problems and then give a heuristic speed-up based on simple deformation of the underlying parametrization of the discriminant. In particular, we focus on the near-circuit case, which means n-variate polynomials with exactly n+3 terms, as well as some related (sparse) square systems. This is joint work with Ellen Chlachidze and Weixun Deng.

J. Maurice Rojas
Texas A&M University
rojas@math.tamu.edu

Ellen Chlachidze
University of Michigan
ellench@umich.edu

Weixun Deng
Texas A&M University
deng15521037237@tamu.edu

MS115

Hybrid Curves and Their Moduli Spaces

This talk provides an introduction to hybrid curves, a new geometric object which mixes Riemann surfaces and graphs, and their moduli spaces. The moduli space of hybrid curves refines the classical DeligneMumford compactification of the moduli space of Riemann surfaces and provides a framwork to answer several analytic questions on asymptotic geometry of degenerating Riemann surfaces (e.g., asymptotics of canonical measures and Green functions). In addition, hybrid curves enjoy analogs of fundamental theorems on smooth compact Riemann surfaces, e.g. a RiemannRoch and AbelJacobi theorem. In this talk, we introduce hybrid curves and overview several recent results. Based on joint work with Omid Amini.

Noema Nicolussi
Universität Potsdam
noema.nicolussi@univie.ac.at

MS115

Realizability of Tropical Pluri-Canonical Divisors

Tropical geometry studies certain discreet, piece-wise linear objects which are supposed to be simplified and distinctly combinatorial analogues of more classical algebro-geometric objects. The relation between the two worlds is the so-called *tropicalization* process: it associates to an algebraic object a tropical one. The classification, which tropical objects arise as the tropicalization of an algebraic one is known as the realizability problem and this question is fundamental to tropical geometry. Understanding realizability is key to an application of tropical geometry to problems from algebraic geometry. In this talk I will present a combinatorial criterion which solves the realizability question for effective tropical pluri-canonical divisors. I will focus on motivation and possible applications to the study of strata of k-differentials. This is joint work with Johannes Schwab.

Felix Röhrle
Universität Tübingen
roehrle@math.uni-frankfurt.de

Johannes Schwab
Goethe Universität Frankfurt
schwab@math.uni-frankfurt.de

MS115

Tropical Geometry and Moduli Spaces: Curves and Vector Bundles

The tropical geometry of algebraic moduli spaces allows us to learn more about the combinatorial structure of their compactifications. This approach usually proceeds in two steps: First construct a tropical analogue of an algebraic moduli space, then identify it with as a tropicalization of its algebraic counterpart (e.g. in the sense of non-Archimedean skeletons). In this talk, I will explain this approach focusing on the case of the moduli space of curves as well as on the moduli space of semistable vector bundles on the Tate curve. As an application, we will exhibit a non-Archimedean analogue of the P=W phenomenon from non-abelian Hodge theory that, beyond the perverse and the weight filtration, involves a third tropical filtration.

Martin Ulirsch
Goethe University Frankfurt am Main
ulirsch@math.uni-frankfurt.de

Andreas Gross
Goethe University Frankfurt
gross@math.uni-frankfurt.de

Inder Kaur
Loughborough University
i.kaur@lboro.ac.uk

Werner Annette
Goethe University Frankfurt
werner@math.uni-frankfurt.de

Dmitry Zakharov
Central Michigan University
zakha1d@cmich.edu

MS116

Cauchy and Lagrange Bounds for Multivariate Polynomials

We are interested in the generalization to multivariate polynomials of the classical bounds on the modulus of the complex roots of univariate polynomials. To any multivariate polynomial, we associate a tropical polynomial with the same support, obtained by applying the trivial valuation to each coefficient. The zero set of this tropical polynomial is a particular tropical hypersurface which constitutes a polyhedral fan. We establish a bound for the distance between the archimedean amoeba of the complex hypersurface associated to the original polynomial and the latter tropical hypersurface. This generalizes the bound of Cauchy. A system of polynomial equations is said to be strongly mixed when the intersection of the tropical hypersurfaces obtained by the above trivial tropicalization procedure is reduced to the zero vector. Then, we obtain bounds for the archimedean amoeba of the complex variety of a strongly mixed system. We finally consider the generalization of the bounds of Fujiwara (1916), Hadamard (1893) and Lagrange (1769), which involve the slopes of the Newton-polygon of the univariate polynomial. To this end, we use a different tropicalization, obtained by applying the log-of-modulus map instead of the trivial valuation, and bound the distance between the archimedean amoeba of a complex hypersurface and the associated tropical hypersurface.

Marianne Akian
INRIA and CMAP, Ecole Polytechnique
marianne.akian@inria.fr

Stéphane Gaubert
INRIA and CMAP, École polytechnique
stephane.gaubert@inria.fr

Gregorio Malajovich
Universidade Federal do Rio de Janeiro
gregorio@im.ufrj.br

MS116

Mixed Volumes, Sparse Resultants and Residues in the Torus

Resultants and residues are basic invariants of systems of polynomial equations. When these systems are sparse, the mixed volume of the input's support polytopes plays a special role in computing these invariants. We will present some interesting interactions among these objects in the context of algebraic elimination theory.

Carlos D'Andrea
Universitat de Barcelona
cdandrea@ub.edu

MS116

The Zonoid Algebra

In this seminar I will discuss the so called ”zonoid algebra”, a construction introduced in a recent work (joint with Breiding, Brgisser and Mathis) which allows to put a ring structure on the set of zonoids (i.e. Hausdorff limits of Minkowski sums of segments). This framework gives a new perspective on classical objects in convex geometry, and it allows to introduce new functionals on zonoids, in particular generalizing the notion of mixed volume. Moreover this algebra plays the role of a probabilistic intersection ring for compact homogeneous spaces.

Antonio Lerario
SISSA (Trieste)
KTH (Stockholm)
lerario@sissa.it

Peter Bürgisser
Technische Universität Berlin
Germany
pbuerg@math.tu-berlin.de

Leo Mathis
University of Frankfurt
Mathis@mathematik.uni-frankfurt.de

Paul Breiding
University Osnabrück
Germany
pbreiding@uni-osnabrueck.de

MS117

Differential Transcendence and Galois Theory

In this talk we consider meromorphic solutions of difference equations and prove that very few among them satisfy an algebraic differential equation. The basic tool is the difference Galois theory of functional equations.

Thomas Dreyfus
Université Lyon 1
dreyfus@math.univ-lyon1.fr

MS117

Seminumeric Factorization of Linear Differential Operators

In analogy with the usual Galois group of a polynomial, you can define the differential Galois group of a linear Ordinary Differential Equation (ODE). This group encodes all the algebraic and/or differential relations between the solutions of the equation. There is a theoretical algorithm for computing it [Hrushovski, 2002] seemingly too complex to be worth implemented. However the numerical evaluation of the solutions provides an efficient way to numerically approach some elements of this group. In 2007, van der Hoeven [van der Hoeven, 2007] proposed to use this for the exact computation of the differential Galois group and he gave a seminumeric algorithm for the factorization of linear ODEs. Here the term ”seminumeric” means that approximate numeric computations are involved although the output is exact. I will present a seminumeric Las Vegas algorithm for factoring Fuchsian ODEs with rational function coefficients [Chyzak, Goyer, Mezzarobba, 2022]. This algorithm combines ideas of van Hoeij's ”local-to-global method” [van Hoeij, 1997] and of the analytic approach proposed by van der Hoeven. It essentially reduces to the former in ”easy” cases where the local-to-global method succeeds, and to an optimized variant of the latter in the ”hardest” cases, while handling intermediate cases more efficiently than both. This is a joint work with Frdric Chyzak and Marc Mezzarobba.

Alexandre Goyer
INRIA Saclay
alexandre.goyer@inria.fr

MS117
Differentially Algebraic Functions

Generating functions are often regarded as power series solutions of ordinary differential equations (ODEs). Perhaps, the most encountered differential equations are the so-called holonomic ones, i.e., linear differential equations with polynomial coefficients. General solutions to holonomic ODEs are differentially finite (D-finite) functions, which have nice closure properties well studied at the interplay between symbolic computations and combinatorics. However, as D-finite functions are not closed under composition and division, one considers ODEs that are multivariate polynomials in the independent variables and derivatives of the dependent ones. We call them algebraic differential equations (ADEs), and their general solutions are called differentially algebraic (D-algebraic) functions. Most known generating functions that involve Bernoulli and Euler numbers in their series expansion are D-algebraic. An interesting discussion on the appearance of D-algebraic functions in combinatorics can be found in [Raschel, Kilian and Bousquet-Mélou, Mireille and Bernardi, Olivier. Counting quadrant walks via Tutte's invariant method. 2020]. We discuss algorithms for the closure properties of D-algebraic functions and present a Maple implementation. This is joint work with Rida Ait El Manssour and Anna-Laura Sattelberger.

Rida Ait El Manssour
MPI MiS Leipzig
rida.manssour@mis.mpg.de

Anna-Laura Sattelberger
KTH Royal Institute of Technology
alsat@kth.se

Bertrand Teguia Tabuguia
Max Planck Institute Leipzig
bertrand.teguia@mis.mpg.de

MS118
Secure Implementations of Isogenies

In the last years, isogenies have caught the attention of cryptographers since they present good properties such as small private and public keys, and it is possible to use almost directly in the Diffie-Hellman protocol. However, they are slower when we compare the isogeny-based schemes against other post-quantum schemes. Furthermore, in a cryptographic context, the computation of isogenies must be secure against side-channel attacks. In this talk, we will talk about the common mistakes when one implements isogeny schemes and how to avoid those mistakes. First, a brief introduction to timing attacks and how to protect the implementation against them. Later, we will check the current fault attacks against isogeny schemes, and countermeasures to ensure safe and efficient implementation.

Gustavo Banegas
Qualcomm, France
gustavo@cryptme.in

MS118
The Algorithmic Deuring Correspondence in Cryptography

The Deuring correspondence is the link between supersingular elliptic curves in characteristic p and maximal orders inside the quaternion algebra ramified at p and infinity. This link has recently found some applications in isogeny-based cryptography and sub-domain of post-quantum cryptography. In this talk, we will present several recent cryptographic constructions and how their design and security is related to effective algorithms to compute the Deuring correspondence. In particular, we will focus on the SQISign and pSIDH protocols.

Antonin Leroux
Inria and Laboratoire dInformatique de lEcole
polytechniqu
antonin.leroux@polytechnique.org

MS118
SQISignHD: New Dimensions in Cryptography

We will present SQISignHD, a new post-quantum digital signature scheme inspired by SQISign. SQISignHD exploits the recent algorithmic breakthrough underlying the attack on SIDH, which allows to efficiently represent isogenies of arbitrary degrees as components of a higher dimensional isogeny. SQISignHD overcomes the main drawbacks of SQISign. First, it scales well to high security levels, since the public parameters for SQISignHD are easy to generate. Second, the signing procedure is simpler and more efficient. Third, the scheme is easier to analyse, allowing for a much more compelling security reduction. Finally, the signature sizes are even more compact than (the already record-breaking) SQISign, with compressed signatures as small as 105 bytes for the post-quantum NIST-1 level of security. These advantages may come at the expense of the verification, which now requires the computation of an isogeny in dimension 4, a task whose optimised cost is still uncertain, as it has been the focus of very little attention.

Pierrick Dartois
Inria Bordeaux Sud-Ouest
pierrick.dartois@u-bordeaux.fr

Antonin Leroux
Inria and Laboratoire dInformatique de lEcole
polytechniqu
antonin.leroux@polytechnique.org

Damien Robert
Inria Bordeaux Sud-Ouest
damien.robert@inria.fr

Benjamin Wesolowski
ENS Lyon
benjamin.wesolowski@ens-lyon.fr

MS119

How to Obtain a Minimal Input-State-Output Representation of a Convolutional Code

A rate k/n convolutional code $\mathcal{C}$ is an $\mathbb{F}[z]$-submodule of rank k of the module $\mathbb{F}[z]^n$, where $\mathbb{F}$ is a finite field. Therefore, there exists $G(z) \in \mathbb{F}[z]^{n\times k}$, of rank k, such that

$$\mathcal{C} = \left\{ \boldsymbol{v}(z) \in \mathbb{F}[z]^n \mid \boldsymbol{v}(z) = G(z)\boldsymbol{u}(z) \text{ with } \boldsymbol{u}(z) \in \mathbb{F}[z]^k \right\}.$$

The convolutional code $\mathcal{C}$ can be described by a time invariant linear system

$$\left.\begin{array}{rcrcr} \boldsymbol{x}_{t+1} & = & A\boldsymbol{x}_t & + & B\boldsymbol{u}_t \\ \boldsymbol{y}_t & = & C\boldsymbol{x}_t & + & D\boldsymbol{u}_t \end{array}\right\}, \ \boldsymbol{v}_t = \begin{bmatrix} \boldsymbol{y}_t \\ \boldsymbol{u}_t \end{bmatrix}, t \geq 0, \ \boldsymbol{x}_0 = \mathbf{0},$$

where $A \in \mathbb{F}^{m\times m}$, $B \in \mathbb{F}^{m\times k}$, $C \in \mathbb{F}^{(n-k)\times m}$ and $D \in \mathbb{F}^{(n-k)\times k}$. We say (A,B,C,D) is an input-state-output (ISO) representation of $G(z)$ of dimension m and it is called minimal if its dimension is δ, the maximum degree of the $k \times k$ minors of $G(z)$. In this talk, from $G(z)$ we obtain a generator matrix and a parity check matrix of a $[2\delta + n, \delta + k]$ block code, which allow us to obtain a minimal ISO representation (A,B,C,D) of $\mathcal{C}$.

Joan-Josep Climent
Universitat d'Alacant
Dep. Ciencia de la Computacio
jcliment@ua.es

Diego Napp, Verónica Requena
Universitat d'Alacant
Departament de Matemàtiques
diego.napp@ua.es, vrequena@ua.es

MS119

Convolutional Goppa Codes over the Erasure Channel

It is well-known that when decoding on the erasure channel MDP codes have optimal properties. Particularly interesting is the class of complete-MDP codes. It is also known that such codes exist for any parameters $[n, k, \delta]$ as long as the field is big enough. Different approaches have been taken in order to estimate the size of the field so that MDP codes can be constructed. Convolutional Goppa codes (CGC) were presented as a generalization in the convolutional setting of algebraic geometric codes. This construction has been shown to provide optimal samples of codes. Later it was shown that in fact any convolutional code might be constructed as a CGC by choosing appropriate rational points and evaluating functions. Our aim is to utilize the Goppa structure of convolutional codes in order to describe MDP codes and explore under which conditions they may exist in such terms.

José Ignacio Iglesias Curto
University of Salamanca
joseig@usal.es

MS119

Low Memory Convolutional Streaming Codes for the Packet Expansion Approach

Packet channels are subject to packet losses and these can be modeled as packet erasures where we know the lost packet's location but not its content. Channel coding provides a way to recover much of this content and thus protect against the impact of packet losses. Modern day communications often requires packets to be sent with high reliability and very little delay. In particular, many modern interactive applications, such as interactive video and telesurgery, involve requirements to optimize latency, throughput and loss rate. In this talk I will present some recent work on low delay streaming codes that are based on low memory convolutional codes. These streaming codes cater for situations where erasures occur in bursts. To prevent congestion, the encoding approach is via packet expansion, so as not to create additional packets. The construction of the streaming codes involves particular interleaving techniques applied to convolutional codes. We show how properties of the low memory convolutional code translate into properties of the streaming code, particularly its decoding delay.

Margreta Kuijper
University of Melbourne
mkuijper@unimelb.edu.au

MS119

On the Decoding of Convolutional Codes over An Erasure Channel

The decoding capacity of convolutional codes over an erasure channel was analyzed in [V. Tomas, J. Rosenthal and R. Smarandache, Decoding of Convolutional Codes Over the Erasure Channel, IEEE Transactions on Information Theory, 58.1 (2012), 90108]. In this paper, the authors considered noncatastrophic convolutional codes and presented a decoding algorithm for these codes using parity-check matrices. We present a decoding algorithm which considers an encoder instead a parity-check matrix and analyze the differences (advantages/disadvantages) between these two decoding algorithms.

Raquel Pinto
University of Aveiro
raquel@ua.pt

MS120

Invariants of q-Polymatroids

An integer polymatroid is defined to be an integer-valued non-negative, increasing, semimodular function f on the power set $\mathcal{P}(S)$ of a finite set S. Invariants of linear codes, such as their binomial moments and weight distributions are actually matroidal invariants and are connected to the characteristic polynomial, rank-generating function, coboundary polynomial and the Tutte polynomial of the underlying matroid. q-Analogues of concepts in the theory of matroids and polymatroids arise by replacing $\mathcal{P}(S)$ with the lattice $\mathcal{L}(V)$ of subspaces of a finite-dimensional vector space V. We consider identities and properties of the characteristic polynomial of a q-polymatroid in terms of some of its minors. We furthermore compute the critical exponents of some classes of matrix codes.

Eimear Byrne
UC Dublin
ebyrne@ucd.ie

Gianira Alfarano
Eindhoven University of Technology
g.n.alfarano@tue.nl

MS120

Tutte Partitions of Q-Matroids

A matroid is a combinatorial object that generalises the notion of independence in a graph or vector space and is defined on a subset (Boolean) lattice. A q-matroid is a generalisation of a matroid, which is defined on a subspace (modular) lattice. The Tutte polynomial is a fundamental graph invariant that was generalised by Crapo in 1969 to be a matroid invariant. In this talk, we provide a construction of the Tutte polynomial for both matroids and q-matroids based on an appropriate partition of the underlying support lattice into intervals that correspond to prime-free minors, which we call a Tutte partition. We show that such partitions in the matroid case include the class of partitions arising in Crapo's definition of the Tutte polynomial, while not representing a direct q-analogue of such partitions. In the second part of this talk, we introduce axioms of q-Tutte-Grothendieck invariance and show that this yields a q-analogue of Tutte-Grothendieck invariance. We establish the connection between the rank polynomial and the Tutte polynomial, showing that one can be obtained from the other by convolution. The new results in this talk are joint work with E. Byrne.

Andrew Fulcher
University College Dublin
Ireland
andrew.fulcher@ucdconnect.ie

Eimear Byrne
UC Dublin
ebyrne@ucd.ie

MS120

The Euler Characteristic and The Mobius Invariant of Matroids and the q-Analogue

For a co-loopless matroid M of rank r, the reduced Euler characteristic of the corresponding matroid complex S_M is determined by a Möbius function via the relation $\chi(S_M) = (-1)^{r-1}|\mu_{L_M}(\hat{0},\hat{1})|$, where L_M is the lattice of cycles of M. The relation can be seen as a link between the poset of independent sets of M, and the geometric lattice of flats of the dual matroid M^*, which has a very interesting application to coding theory. It has been shown that the generalized Hamming weights of a linear code can be determined by Betti numbers of the Stanley-Reisner ring of an associated matroid. In this talk, I will present a q-analogue of this relation where one consider the Euler characteristic of the order complex associated to a q-matroid. I will also briefly discuss its potential application to the theory of rank metric codes.

Rakhi Pratihar
Inria Saclay Centre
France
pratihar.rakhi@gmail.com

MS120

On the Shellability of Some Chain Complexes from Ranked Lattices

A well known result says that all matroid complexes are shellable. Recently, in the q-analogue setting, it was shown that q-matroid complexes formed by independent spaces of q-matroids are q-shellable. The notion of q-shellability partially helped to understand the topological property of a q-matroid complex. In a separate work, we showed that the q-shellability of a q-complex implies the shellability of the chain complex (which is a simplicial complex) defined by the q-complex. In this talk, I explain how this result can be generalized to a more general class of ranked lattice. We introduce the notion of shellability of subposets of a so-called ”power-lattices” and we show that if the subposet is ”shellable”, then the chain complex defined by this subposet is also shellable as a simplicial complex.

Tovohery H. Randrianarisoa
Umea University
Sweden
tovohery.randrianarisoa@umu.se

MS121

Logarithmic Voronoi Cells for Gaussian Models

Logarithmic Voronoi cells are convex sets that arise in algebraic statistics as pre-images of maximum likelihood estimation. For Gaussian models, each logarithmic Voronoi cell is contained in its log-normal spectrahedron. My talk will introduce the two sets, and we will see that for both directed and undirected graphical models they coincide. For the latter family, I will introduce a decomposition theory of logarithmic Voronoi cells. We will also study covariance models, for which logarithmic Voronoi cells are, in general, strictly contained in log-normal spectrahedra. We will look at the bivariate correlation model in detail. This talk is based on joint work with Serkan Hosten.

Yulia Alexandr
UC Berkeley
yalexandr@berkeley.edu

Serkan Hosten
Department of Mathematics
San Francisco State University
serkan@sfsu.edu

MS121

Expectation of a Random Submanifold

In a joint work with Michele Stecconi, we study the zero set of a nice enough random smooth function. We show how to compute the expectation of the Riemannian volume of such zero sets. This computation involves a family of convex bodies (zonoids) in the exterior powers of the cotangent bundle. I will explain this construction and how this is linked to the recently introduced zonoid algebra (j.w. with Breiding Brgisser and Lerario). If times allows, I will show how this theory gives rise to Crofton formulae in Finsler geometry.

Leo Mathis
University of Frankfurt

Mathis@mathematik.uni-frankfurt.de

MS121

Average Degree of the Essential Variety

The essential variety is an algebraic subvariety of dimension 5 in $\mathbb{R}P^8$, which appears in Computer Vision. The degree of this variety is 10, so there can only be a maximum of 10 complex solutions. We compute the expected number of real points in the intersection of the essential variety with a random linear space of codimension 5. In this talk, my aim is to show how convex geometry aids in these computations. I will introduce the essential Zonoid and we will see how its support function gives the expected number of real solutions for a certain distribution. This is joint work with Paul Breiding, Samantha Fairchild and Pierpaola Santarsiero.

Elima Shehu
MPI MiS Leipzig and University of Osnabrück
elima.shehu@mis.mpg.de

Paul Breiding
University Osnabrück
Germany
pbreiding@uni-osnabrueck.de

Samantha Fairchild
MPI MiS Leipzig
skayf92@gmail.com

Pierpaola Santarsiero
University of Trento
pierpaola.santarsiero@mis.mpg.de

MS121

Fiber Bodies of Spectrahedra

Given a linear map on the vector space of symmetric matrices, every fiber intersected with the set of positive semidefinite matrices is a spectrahedron. Using the notion of the fiber body we can build the average over all such fibers and thereby construct a compact, convex set, the fiber body. We show how to determine the dimensions of faces and normal cones to study the boundary structure of the fiber body given that we know about the boundary of the fibers. We use this to study the fiber body of Gram spectrahedra in the case of binary sextics and ternary quartics and find a large amount of structure on the fiber body. We prove that the fiber body in the case of binary sextics has exactly one face with a full-dimensional normal cone, whereas the Gram spectrahedron of a generic positive binary sextic has four such points. The fiber body in the case of ternary quartics changes drastically.

Julian Vill
OvGU Magdeburg
julian.vill@ovgu.de

MS122

Harmonic Hierarchies for Polynomial Optimization on Homogeneous Spaces

The aim of this talk is to describe the fundamental components of a novel method for polynomial optimization on the n-sphere by means of polyhedral hierarchies. I will briefly introduce spherical cubature rules, harmonic analysis of polynomials and averaging operators. Afterwards, all these ingredients will come together in a method for computing lower bounds for polynomial minimization on the n-sphere. I will also discuss the framework (rooted in representation theory) in which one can reproduce this method in more general homogeneous spaces, those associated to Gelfand pairs.

Sergio Cristancho, Mauricio Velasco
Universidad de los Andes
se.cristancho@uniandes.edu.co,
m.velasco@uniandes.edu.co

MS122

On the Computational Complexity of the Moment-Sos Hierarchy

The moment-sum-of-squares (moment-SOS) hierarchy is one of the most celebrated and widely applied methods for approximating the minimum of an n-variate polynomial over a feasible region defined by polynomial (in)equalities. A key feature of the hierarchy is that, at a fixed level, it can be formulated as a semidefinite program of size polynomial in the number of variables n. Although this suggests that it may therefore be computed in polynomial time, this is not necessarily the case. Indeed, as O'Donnell (2017) and later Raghavendra & Weitz (2017) show, there exist examples where the sos-representations used in the hierarchy have exponential bit-complexity. We study the computational complexity of the moment-SOS hierarchy, complementing and expanding upon earlier work of Raghavendra & Weitz (2017). In particular, we establish algebraic and geometric conditions under which polynomial-time computation is guaranteed to be possible.

Sander Gribling
IRIF Paris University
gribling@irif.fr

Sven C. Polak
CWI
s.c.polak@tilburguniversity.edu

Lucas Slot
ETH Zurich
lucas.slot@inf.ethz.ch

MS122

Convergence Analysis of Non-Sos Hierarchies for Polynomial Optimization

We provide a convergence analysis of recently proposed non-SOS hierarchies for polynomial optimisation. These hierarchies are similar to Laserre's hierarchy. However, instead of sums of squares (SOS), they are based on other sets of non-negative polynomials such as SOMS, DSOS, SDSOS, SONC and SAG polynomials. A non-SOS version of Putinar Positivstellensatz guarantees the convergence of such hierarchies. We obtain a quantitative version of this non-SOS Positivstellensatz, which implies bounds on the convergence rate of the hierarchy to the global optimum of the polynomial optimisation problem.

Lorenz M. Roebers
Tilburg University
l.m.roebers@tilburguniversity.edu

Juan C. Vera
Tilburg School of Economics and Management
Tilburg University

j.c.veralizcano@tilburguniversity.edu

MS122

The Sonc Cone: Primal and Dual Perspectives

Solving polynomial optimization problems requires to certify nonnegativity of multivariate, real polynomials. A classical way to do this are sums of squares (SOS). An alternative way are sums of nonnegative circuit polynomials (SONC), which I introduced joint with Sadik Iliman in 2014 building on work by Bruce Reznick. For a fixed support, SONCs form a convex cone, which has the same dimension as the corresponding nonnegativity cone. Moreover, motivated from dualization, one can obtain a particular (strict but full-dimensional) subcone of the SONC cone - the DSONC cone - leading to certificates which have, despite being weaker than SONC, the benefit to be obtainable via linear programming. In this talk I will speak about the SONC cone and its DSONC subcone. It is based on joint work Janin Heuer; see ArXiv 2204.03918.

Timo de Wolff
Technische Universität Braunschweig
t.de-wolff@tu-braunschweig.de

Janin Heuer
Institut für Analysis und Algebra
TU Braunschweig
janin.heuer@tu-braunschweig.de

MS123

Polynomial Dynamical Systems and Reaction Networks: Persistence and Global Attractors

The mathematical analysis of global properties of dynamical systems with polynomial right-hand side can be very challenging (for example: the second part of Hilberts 16th problem, or the analysis of chaotic dynamics in the Lorenz system). On the other hand, any dynamical system with polynomial right-hand side can essentially be regarded as a model of a reaction network. Key properties of reaction systems are closely related to fundamental results about global stability in classical thermodynamics. For example, the *Global Attractor Conjecture* (which says that reaction systems that obey some algebraic identities must have very simple dynamics: all solutions must converge to globally attracting fixed points) can be regarded as a finite dimensional version of Boltzmanns H-theorem. We will discuss some of these connections, as well as the introduction of *toric differential inclusions* as a tool for proving the Global Attractor Conjecture. We will also discuss some implications for the more general *Persistence Conjecture* (which says that solutions of any weakly reversible system cannot ”go extinct”), as well as some applications to biochemical mechanisms that implement noise filtering and cellular homeostasis.

Gheorghe Craciun
Department of Mathematics, University of
Wisconsin-Madison
craciun@wisc.edu

MS123

Beyond Boolean Networks

I will present joint work that is an invitation to model biological networks with any finite number m of states for every node; in particular, to predict the qualitative behavior of gene regulatory networks. To model the dynamics, we represent each transition function via operations used in multivalued logic, which are intuitive and close to biological interpretations. We generalize several properties of Boolean networks (the case $m = 2$) and we give an algorithm to compute the fixed points of the system, including some complexity considerations.

Alicia Dickenstein
Universidad de Buenos Aires
alidick@dm.uba.ar

Juliana Garcia Galofre
Universidad de San Andrés, Argentina
jgarciagalofre@udesa.edu.ar

Mercedes Perez Millan
Universidad de Buenos Aires
mpmillan@dm.uba.ar

Reinhard C. Laubenbacher
University of Florida
Department of Medicine
reinhard.laubenbacher@medicine.ufl.edu

MS123

Multistationarity of Rank-One Reaction Networks

The existence of multiple positive steady states in models of reaction networks, referred to as multistationarity, underlies switching behavior in biochemistry, and has been an important area of study for a number of years. A recent approach to multistationarity of large networks relies on lifting positive steady states from smaller network components which are themselves multistationary. This intensified the effort of cataloging small multistationary network structures (multistationary motifs). In this talk we characterize the class of multistationary mass-action networks with 1D stoichiometric subspace, answering a conjecture by Joshi and Shiu.

Casian Pantea, Galyna Voitiuk
West Virginia University
cpantea@math.wvu.edu, galvoit@gmail.com

MS123

Saddle-Node Bifurcations in Chemical Reaction Networks

Saddle-node bifurcations stand at the gate of parameter areas where the coexistence of multiple steady-states (multistationarity) occurs. The identification of saddle-node bifurcations is thus a valuable tool for detecting multistationarity in biochemical systems, a phenomenon of recognized importance in many biological processes. In this talk, we address positive steady-states of ODEs systems arising from chemical reaction networks and we present abstract network conditions that guarantee the occurrence of saddle-node bifurcations. Our approach is function-free: we do not fix a priori the choice of the kinetics and our conditions are solely based on the stoichiometry of the reactions. As a concrete example of application, we explicitly identify the proper bifurcation parameters for Michaelis-Menten and Hills kinetics.

Nicola Vassena
Free University Berlin

nicola.vassena@uni-leipzig.de

MS124

The Geometry of Gaussian Double Markovian Distributions

Gaussian double Markovian models consist of covariance matrices with specified zeros and specified zeros in their inverses. Geometrically, these are intersections of graphical models with inverse graphical models. We describe the semi-algebraic geometry of these models, in particular their dimension, smoothness, connectedness, and vanishing ideals. We give a geometric proof of an exponential family heuristic for a smoothness criterion of Zwiernik. We also continue investigations of singular loci initiated by Drton and Xiao. This is joint work with Tobias Boege, Andreas Kretschmer, and Frank Rttger

Thomas Kahle
OvGU Magdeburg
thomas.kahle@ovgu.de

MS124

Learning Cyclic Linear Non-Gaussian Causal Models

In this talk we will discuss the problem of learning the directed graph for a linear non-Gaussian causal model. Here we do not impose an acyclicity assumption on the unknown directed graph. While in the acyclic case, the directed graph can be found uniquely, when cycles are allowed the graph can be learned up to an equivalence class. We give a description of all the graphs that each equivalence class consists of. We then give an algorithm based on relationships among the second and third order moments of the random vector that recovers the graph, assuming that the graph lies in the family of directed graphs whose strong components are simple directed cycles. This is joint work with Mathias Drton, Marina Garrote-Lopez, and Niko Nikov.

Elina Robeva
University of British Columbia
erobeva@math.ubc.ca

MS124

Causal Inference in Directed, Possibly Cyclic, Graphical Models

In this talk, we consider the problem of learning the Markov equivalence class of a directed graph G from the observational data arising from a distribution in the graphical model of G. We assume that the distribution is *faithful* to the graph G, but do not rely on any further assumptions regarding the graph. In particular, we allow for directed cycles in G. Given the set of conditional independence statements satisfied by the distribution, we correspond a certain score to any partially ordered partition of the vertices of G. Then we greedily search for the partially ordered partitions with the optimal score. We prove that any such partition determines particular structures in the graph that uniquely characterize the Markov equivalence class of G. Moreover, we propose an algorithm for constructing a graph in the Markov equivalence class of G using the optimal partially ordered partitions. This algorithm comes in two versions. While based on experimental evidence, we conjecture that the more efficient version is correct, we prove that the other version is indeed correct. This talk is based on joint work with Elina Robeva.

Pardis Semnani
Department of Mathematics
University of British Columbia
psemnani@math.ubc.ca

MS124

Graphical Representations for Algebraic Constraints of Linear Structural Equations Models

The observational characteristics of a linear structural equation model can be effectively described by polynomial constraints on the observed covariance matrix. However, these polynomials can be exponentially large, making them impractical for many purposes. It turns out that a far more succinct graphical notation can also represent many of these polynomial constraints. I will discuss some of its properties in this talk.

Thijs van Ommen
Utrecht University
m.vanommen1@uu.nl

MS125

Discreteness of Asymptotic Slice Rank and Asymptotic Subrank

Christandl, Gesmundo and Zuiddam (2022) showed that over any field, the asymptotic sub- and slice ranks of any 3-tensor equals 0, 1, or $2^{h(1/3)}$ (where h is the binary entropy function) or is at least 2. In this talk, I will discuss basic properties of the matrix spaces spanned by the slices of 3-tensors that imply that in fact, for certain classes of tensors and fields, the whole spectrum of asymptotic sub- and slice ranks is discrete (has no accumulation points). Based on joint work with Matthias Christandl, Itai Leigh, Amir Shpilka and Jeroen Zuiddam

Jop Briët
Centrum Wiskunde & Informatica
j.briet@cwi.nl

MS125

When are Radicals of Symmetric Ideals Monomial?

Given a polynomial $f \in K[x_1, \ldots, x_n]$ over an algebraically closed field K, we can ask about the common solutions to all permutations of f (by elements of the symmetric group on n letters, permuting the variables in the obvious way). Fixing a set of monomials $\mathcal{A}$ that are allowed to appear in f, we can ask how this symmetrized vanishing set looks like for a general f with support set $\mathcal{A}$. Experimentally, in many cases this set is extremely simple. I will try to make this intuition precise during the talk, and I will indicate the proof of a special case under hypotheses on $\mathcal{A}$. If time permits, I will also mention joint work in progress with Sebastian Debus on Invariant Hilbert schemes of affine space for the natural action of the symmetric group.

Andreas Kretschmer
OvGU Magdeburg
andreas.kretschmer@ovgu.de

MS125

Equivariant Algebraic and Semi-algebraic Geome-

try of Infinite Affine Space

We study Sym(∞)-orbit closures of not necessarily closed points in the Zariski spectrum of the infinite polynomial ring $\mathbb{C}[x_{ij} : i \in \mathbb{N},\ j \in [n]]$. Among others, we characterize invariant prime ideals in this ring. Furthermore, we study projections of basic equivariant semi-algebraic sets defined by Sym(∞) orbits of polynomials in $\mathbb{R}[x_{ij} : i \in \mathbb{N},\ j \in [n]]$. For $n = 1$ we prove a quantifier elimination type result which fails for $n > 1$.

Cordian Riener
UiT The Arctic University of Norway
cordian.riener@uit.no

Mario Kummer
Technische Universität Dresden
mario.kummer@tu-dresden.de

MS125

Covariance Matrices of Length Power Functionals of Random Geometric Graphs

Asymptotic properties of a vector of length power functionals of random geometric graphs, which arise as the 1-skeleton of considered random simplicial complexes, are investigated. More precisely, its asymptotic covariance matrix is studied as the intensity of the underlying homogeneous Poisson point process increases. This includes a consideration of matrix properties like rank, definiteness, determinant, eigenspaces or decompositions of interest. For the formulation of the results a case distinction is necessary. Indeed, in the three possible regimes the respective covariance matrix is of quite different nature which leads to different statements. This talk is based on joint work with Matthias Reitzner and Tim Rmer (Universitt Osnabrck).

Mandala Von Westenholz
Universität Osnabrück
mvonwestenho@uni-osnabrueck.de

MS126

A Sagbi Basis Algorithm

Let R be a polynomial ring over a field endowed with a monomial order and A a subalgebra of R. The initial monomials of the elements of A are the vector space basis of the initial algebra in(A). A subset B of A is a Sagbi basis of A if the initial monomials of the elements of B generate in(A). In contrast to Grbner bases for ideals, Sagbi bases cannot always chosen finite. If it is finite, the monomial algebra in(A) is a toric deformation of A. Sagbi bases are computed by an analogue of the Buchberger algorithm. Starting from a given set B' of generators of A, the goal is to extend the candidate B' repeatedly by further elements if not all binomial relations of the initial monomials of B' can be lifted to relations of B'. The analogue of the Buchberger S-polynomial is a tete-a-tete, and the analogue of reduction is subduction. We have implemented the algorithm in a Singular library. For the combinatorial computations it falls back on Normaliz (version 3.10.0 or newer). We provide 3 variants: a general version (Gen), a version (Deg) proceeding degree by degree, and a version (Hilb) exploiting the Hilbert series of A if it should be known. The implementation is much more efficient than the library sagbi.lib distributed with Singular or the package SubalgebraBases.m2, version 1.1, of Macaulay2. We report on joint work with Aldo Conca (arXiv:2302.14345).

Winfried Bruns
University of Osnabrück
wbruns@uos.de

MS126

A Direttissimo Algorithm for Equidimensional Decomposition

We describe a recursive algorithm that decomposes an algebraic set into locally closed equidimensional sets, i.e. sets which each have irreducible components of the same dimension. At the core of this algorithm we put our own spin on a classical incremental solving strategy and work with Grbner bases to encode locally closed equidimensional sets. Equipped with this, our algorithm avoids generic projections and other genericity assumptions on the input frequently made when decomposing polynomial systems such as Noether position. Built around the philosophy to split a given polynomial system as often as possible, as irredundantly as possible, our algorithm is both simple to describe and implement and produces fine decompositions on more structured systems where ensuring genericity assumptions often destroys the structure of the system at hand. The algorithm has been implemented using the computer algebra system OSCAR with the additional enhancement of a certain probabilistic data structure. Experimental results indicate that it is able to tackle some polynomial systems which are out of reach of other algorithms for equidimensional decomposition available in state-of-the-art computer algebra systems. This is joint work with Christian Eder, Pierre Lairez and Mohab Safey El Din.

Rafael Mohr
RPTU Kaiserslautern-Landau
LIP6 - Sorbonne Université
rafael.mohr@lip6.fr

MS126

Tropical Geometry of Parametrized Polynomial Systems

In this talk, we discuss how tropical geometry can help in solving parametrised polynomial systems for generic choices of parameters. We begin with a generalisation of Bernstein's Theorem from systems with fixed monomial supports to general parametrised systems. Herein, the mixed volume is replaced by the tropical intersection product and the algebraic condition on the facial systems is replaced by a combinatorial condition on the intersection of tropical varieties. We show how the generalised theorem can be applied to the steady state equations of any chemical reaction network, and derive an algorithm that computes the number of (complex) steady states. This number can either serve as a certificate that all solutions have been found via monodromy, or - as it is a tropical intersection number - be used to create a generalisation of polyhedral homotopies. We conclude the talk with an outlook on systems with fixed polynomial supports as studied by Kaveh and Kovanksii, and an algorithm to compute the volume of any Newton Okounkov body. This is joint work with Elisenda Feliu, Paul Helminck, Oskar Henriksson, Benjamin Schroeter, and Mate Telek.

Yue Ren
Durham University

yue.ren2@durham.ac.uk

MS126

Using Signature Grbner Bases to Find Short Ideal Representations

Grbner bases have been developed for solving the ideal membership problem, and have since proven useful in a wide range of other applications, notably for solving polynomial systems. In other settings, they have retained their original purpose regarding the ideal membership problem. In particular, in the non-commutative case, they have been used for proving identities in operator algebras: a given expression is an identity if and only if it belongs to the ideal spanned by the relations between the generators of the algebra. In recent years, Grbner bases have seen the development of the new paradigm of signatures, which have been used both for optimizing the algorithms, and for extracting additional information on the ideal, in particular regarding the module of syzygies and the cofactor representation of the generators. In the context of proof of identities, it makes it possible to produce explicit proofs, and in particular certify the output of the Grbner basis computation. In this work, we show that the data provided by signature Grbner basis algorithms can also be used to find short proofs of known identities. Namely, we show that this problem reduces to the classical problem of finding sparse solutions of linear systems, and that practical instances are within reach of existing LP solvers. (Joint work with Clemens Hofstadler)

Thibaut Verron
Institute for Algebra, Johannes Kepler University
Altenbergerstraße 69, 4040 Linz, Austria
thibaut.verron@jku.at

MS127

Tropical Compactifications of Realization Spaces of Matroids

In this talk, we are going to introduce matroids and their realization spaces. These are moduli spaces parametrizing configurations of points in projective spaces, whose independence is prescribed by the bases of the underlying matroid. The tropical compactification of these spaces is especially relevant, because it is related to many other celebrated constructions, but it can be defined and understood in a more combinatorial way. For instance, the realization space of the uniform matroid of rank 2 on n elements corresponds to $M_{0,n}$ and its tropical compactification to $\overline{M_{0,n}}$.

Laura Casabella
MPI MiS
laura.casabella@mis.mpg.de

MS127

Irreducibility of Severi Varieties via Tropical Geometry

In this talk, I will explain how the theory of tropical curves can be used to show irreducibility of some classical moduli spaces, in particular that of Severi varieties. As an application, one obtains irreducibility also for the moduli space of (abstract) curves of fixed genus, as well as for the Hurwitz schemes. This is joint work with Ilya Tyomkin and Xiang He.

Karl Christ
Leibniz University Hannover, Germany
kchrist@math.uni-hannover.de

MS127

The Logarithmic Hilbert Scheme and Its Tropicalisation

The logarithmic Hilbert scheme is the first example of the logarithmic Quot scheme. A tropical version of a Hilbert scheme plays a crucial role in constructing and understanding logarithmic Quot schemes. This talk will focus on toric varieties called logarithmic linear systems. These are logarithmic analogues of the moduli space of divisors on a toric variety. The fans of logarithmic linear systems are closely related to secondary polytopes and also to moduli spaces of tropical hypersurfaces.

Patrick Kennedy-Hunt
University of Cambridge
pfk21@cam.ac.uk

MS128

Reduction Systems and Degree Bounds for Integration

In symbolic integration, the Risch-Norman algorithm tries to find the closed forms of elementary integrals over differential fields based on heuristic degree bounds. Norman presented an approach that avoids degree bounds and only relies on the completion of reduction systems. We give a formalization of complete reduction systems and develop a refined algorithm with a proof of correctness, which terminates in more instances. In some situations, when the algorithm cannot terminate, we can also find infinite reduction systems that are complete. We present such infinite systems for the fields generated by Airy functions, complete elliptic integrals, and solutions of certain second-order linear differential equations, respectively. Moreover, complete reduction systems can be used to find rigorous degree bounds. We give a general formula for the weighted degree bounds and also find tight bounds for above examples.

Hao Du
Beijing University of Posts and Telecommunications (BUPT)
haodu@bupt.edu.cn

Clemens Raab
Johannes Kepler University Linz (JKU)
clemensr@algebra.uni-linz.ac.at

MS128

Characteristic Singularities of (in)finite Equation Systems

Decompositions of combinatorial structures translate very often to functional equations with positive coefficients for their generating functions. A theorem by Bender (1974) says that if the generating function is univariate and the equation not linear, the generating function always has a dominant square root singularity - which in turn means that its coefficients grow asymptotically at the rate $cn^{-3/2}R^n$, where c and R are suitable constants. The result extends to strongly connected finite systems of equations but for weakly connected or infinite systems we can observe a broader variety of singularities appearing. In this talk, we will give an overview of functional equations systems and their singular behaviour and discuss combinatorial applications.

Eva-Maria Hainzl
TU Wien
eva-maria.hainzl@tuwien.ac.at

MS128

(-1)-Enumerations of Arrowed Gelfand-Tsetlin Patterns

Arrowed Gelfand-Tsetlin patterns have recently been introduced to study alternating sign matrices. In this paper, we show that a (-1)-enumeration of arrowed Gelfand-Tsetlin patterns can be expressed by a simple product formula. The numbers are a one-parameter generalization of the numbers $2^{n(n-1)/2}\prod_{j=0}^{n-1}\frac{(4j+2)!}{(n+2j+1)!}$ that appear in recent work of Di Francesco. A second result concerns the (-1)-enumeration of arrowed Gelfand-Tsetlin patterns when excluding double-arrows as decoration in which case we also obtain a simple product formula. We are also able to provide signless interpretations of our results. The proofs of the enumeration formulas are based on a recent Littlewood-type identity, which allows us to reduce the problem to the evaluations of two determinants. The evaluations are accomplished by means of the LU-decompositions of the underlying matrices, and an extension of Sister Celine's algorithm as well as creative telescoping to evaluate certain triple sums. In particular, we use implementations of such algorithms by Koutschan, and by Wegschaider and Riese.

Florian Schreier-Aigner
University Vienna
florian.schreier-aigner@univie.ac.at

Ilse Fischer
University of Vienna
ilse.fischer@univie.ac.at

PP1

Solving Equations on Parameterized Varieties

In this poster we present a new algorithm to solve structured polynomial equations over an algebraically closed field. The algorithm is based on eigenvalue computations. We assume that the equations are defined on a unirational variety and specialize the construction of Macaulay matrices to this setting. When the parameterizing functions form a Khovanskii basis, these matrices can be computed in a nice combinatorial way. This plays a fundamental role in the implementation. To the best of our knowledge, Khovanskii bases had not been used in symbolic equation solving before. We illustrate our algorithm by solving equations on del Pezzo surfaces and Grassmannians.

Barbara Betti, Marta Panizzut, Simon Telen
MPI MiS Leipzig
barbara.betti@mis.mpg.de, marta.panizzut@mis.mpg.de;, simon.telen@mis.mpg.de;

PP1

Parametric Positive Toricity of Steady State Varieties

Monomial parametrizability (also called *toricity*) of the solutions of polynomial system plays an important role in many applications. For instance, checking whether a given reaction network has various chemical properties such as multistationarity simplifies greatly under the assumption of toricity of the set of steady states, provided that the exponents of the parametrization are known. Over the complex numbers, toricity in the above sense is well understood, but in reaction network theory, the situation is complicated by the fact that only the positive steady states are relevant. In addition, one often wants to check toricity for all possible values of certain unknown parameters called rate constants that appear in the polynomials. Previous work on this type of *parametric positive toricity* in the network-theoretic context has mainly focused on various sufficient algebraic and graph-theoretic conditions. In this work, we give new conditions for both detecting and precluding parametric positive toricity for any system consisting of linear combinations of monomials scaled by positive parameters. Along the way, we invoke a wide array of concepts from computational and real algebraic geometry, including polyhedral geometry, homotopy continuation, injectivity of monomial maps on linear subspaces, and the interplay between a complex variety and its real part. This is joint work with Elisenda Feliu.

Oskar Henriksson, Elisenda Feliu
University of Copenhagen
oskar.henriksson@math.ku.dk, efeliu@math.ku.dk

PP1

Hilbert Functions and Tensor Decomposition

A fundamental problem in computational algebraic geometry is solving systems of homogeneous polynomial equations with finitely many solutions. The complexity of this problem strongly depends on the Hilbert function of the ideal generated by the equations. In applications, these ideals are often not saturated, but rather strictly contained in the vanishing ideal. This happens, for instance, in tensor decomposition, where we are handed only the generators in a low degree. We study the Hilbert function in such cases and deduce complexity results on eigenvalue methods for these problems. Our questions relate to classical problems such as the ideal generation conjecture.

Leonie Kayser
Max Planck Institute for Mathematics in the Sciences
Inselstraße 22, 04103 Leipzig, Germany
leo.kayser@mis.mpg.de

Simon Telen
MPI Leipzig
simon.telen@mis.mpg.de

Fulvio Gesmundo
University of Saarland
gesmundo@cs.uni-saarland.de

PP1

Identifying Trace Affine Linear Sets Using Homotopy Continuation

We investigate how the coefficients of a sparse polynomial system influence the sum, or the trace, of its solutions. We discuss an extension of the classical trace test in numerical algebraic geometry to sparse polynomial systems. Two known methods for identifying a trace affine linear subset of the support of a sparse polynomial system use sparse resultants and polyhedral geometry, respectively. We introduce a new approach which provides more precise classifications of trace affine linear sets than was previously known. For this new approach, we developed software in Macaulay2.

Julianne Mckay
Clemson University
mckay6@clemson.edu

PP1

High Dimensional Functional Data Analysis via Algebraic Geometry

When regressing high-dimensional functional data, challenges are often encountered mainly for the in-sample than out-sample results, and even worse when subjected to the curse of dimensionality. For example, on the in-sample, minimal bounds on the eigenvalues of the covariance matrix for the covariates, when using ridge regression are not generally considered. This study aims to explore the in-sample MSPE properties of different regression methods (except ridge regression) and understand whether the eigenvalue lower bounding conditions are generally avoidable in high-dimensional Hilbert settings.

Leonard Mushunje
Midlands State University
leonsmushunje@gmail.com

PP1

Neural Networks and Discriminant Loci of Parameterized Polynomial Systems

Parameterized polynomial systems are ubiquitous in applications. When the solution set of the parameterized system of equations has dimension 0, consisting of finitely many points, the number of solutions is locally constant outside a proper algebraic variety known as the discriminant. While the discriminant can be computed symbolically using Grbner basis methods, this is often intractable even in small cases. We instead characterize the discriminant locus as the decision boundary of a supervised classification problem in machine learning, where the goal is to classify the real root structure of parameters. We consider approximations of the discriminant of the quadratic equation by traditional neural networks and neural networks with polynomial activation functions and show that the decision boundaries of our neural network recover the quadratic discriminant with high numerical accuracy. We also discuss applications of our methods to larger parameterized polynomial systems.

Wern Juin Gabriel Ong
Bowdoin College
gong@bowdoin.edu

Anna Seigal
Harvard University, U.S.
aseigal@seas.harvard.edu

PP1

Modeling the Probability of Sufficient Data for Graphical Lasso Maximum Likelihood Estimates

Associated to each graph G is a Gaussian graphical model. Such models are often used in high-dimensional settings, i.e. where there are relatively few data points compared to the number of variables. The maximum likelihood threshold of a graph is the minimum number of data points required to fit the corresponding graphical model using maximum likelihood estimation. Graphical lasso is a method for selecting and fitting a graphical model. In this project, we ask: when graphical lasso is used to select and fit a graphical model on n data points, how likely is it that n is greater than or equal to the maximum likelihood of the corresponding graph?

Hayden K. Outlaw, Daniel Bernstein
Tulane University Mathematics Department
houtlaw@tulane.edu, dbernstein1@tulane.edu

PP1

Likelihood Geometry and Statistics for Quasi-Independence Models

Quasi-independence models are a family of statistical models that are used to describe multi-way (or k-way) relationships between discrete-valued random variables, within the purview of identified constraints. Here the integer k is the dimension of the model. We consider the maximum likelihood estimators (MLEs) of objective functions associated with such quasi-independence models and provide an algorithm that allows for the simplification of the computation of such MLEs associated with models of dimension in excess of 2. We express the MLE of a quasi-independence model in terms of MLEs of only 2-way models, by using the existing literature on toric fibre products. Specifically, in our work, we use the symmetric property of the natural product of MLEs under the toric fibre product, to invert the relevant toric fibre products, such that potential toric fibre factors of a given model are identified for the first time. We also provide a related criterion for the maximum likelihood degree (ML-degree) of a k-way quasi-independence model to be 1, as is often desired. Here we use a pre-existing condition on the bipartite graph of a 2-way quasi-independence model with ML-degree 1.

Niharika Paul
University of Oxford, United Kingdom
niharika.paul@exeter.ox.ac.uk

Heather Harrington
Mathematical Institute
University of Oxford
harrington@maths.ox.ac.uk

Jane Ivy Coons
Universty of Oxford
jane.coons@sjc.ox.ac.uk

PP1

Computing Models of Del Pezzo Surfaces in P1 X P1 X P1 Format

We construct two types of wellformed and quasismooth biregular models (infinite series) of rigid orbifold del Pezzo surfaces having their (sub) anti-canonical embeddings in $\mathbb{P}^6(w_i)$. One type has a family of rigid del Pezzo surfaces for varying sets of weights of $\mathbb{P}^6(w_i)$ and has a fixed Fano index and the second type has a family for each varying set of weights and Fano index I: In the first case, the set of weights and in the second case both sets of weights and Fano indices are parameterized by the set of positive integers. The equations describing their images under (sub) anti-canonical embeddings are given in terms of the equations of the Segre embedding of $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$, which have codimension 4 in $\mathbb{P}^7$. We distinguish those models which can not be deformed to a toric variety.

Muhammad I. Qureshi

King Fahd University of Petroleum and Minerals
imran.qureshi@kfupm.edu.sa

PP1

The Structure of the Moduli Spaces of Toric Dynamical Systems

We consider complex balanced mass-action systems, also called toric dynamical systems. They are polynomial dynamical systems arising from reaction networks and have remarkable dynamical properties. We study the topological structure of their moduli spaces (i.e., the toric locus). First we show that the complex balanced equilibria depend continuously on the parameter values. Using this result, we prove that the moduli space of any toric dynamical system is connected. In particular, we emphasize the product structure of the moduli space: it is homeomorphic to the product of the set of complex balanced flux vectors and the affine invariant polyhedron. This is joint work with Gheorghe Craciun and Jiaxin Jin.

Gheorghe Craciun
Department of Mathematics, University of
Wisconsin-Madison
craciun@wisc.edu

Jiaxin Jin
The Ohio State University
jin.1307@osu.edu

Miruna-Stefana Sorea
SISSA, Trieste and RCMA ULBS
SISSA, Trieste and RCMA ULBS
miruna.stefana.sorea2019@gmail.com