

FOCM 2014 - Workshop A6

Real Number Complexity

A6 - December 11, 14:30 – 15:00

SOME RESULTS ON THE COMPLEXITY OF THE EIGENVALUE PROBLEM

Diego Armentano

Universidad de La República, Uruguay
diegoax@gmail.com

In this talk we present an algorithm for the eigenvalue(eigenvector) problem which runs on average polynomial time over the space of n by n complex matrices with Gaussian entries.

Joint work with Carlos Beltrán (Universidad de Cantabria, Spain), Peter Bürgisser (Technische Universität Berlin, Germany), Felipe Cucker (City University of Hong Kong, Hong Kong) and Michael Shub (City University of New York, USA).

A6 - December 11, 15:00 – 15:30

ON SPARSE POLYNOMIAL SOLVING

Gregorio Malajovich

Universidade Federal do Rio de Janeiro, Brasil
gregorio.malajovich@gmail.com

Most of the rigorous theory of path-following algorithms for polynomial system solving assumes dense or dense multi-homogeneous polynomial systems. However, typical examples arising from applications tend to have a sparse structure which calls for theorems.

I will report on recent advances on sparse polynomial solving by homotopy, including mixed volume computation and path-following on toric varieties.

A6 - December 11, 15:35 – 16:25

VARIATIONAL ANALYSIS IN THE LIGHT OF SEMI-ALGEBRAIC GEOMETRY

Aris Daniilidis

Universidad de Chile, Chile
arisd@dim.uchile.cl

In this talk we survey results of the so-called Semi-algebraic (Tame) Variational Analysis, with emphasis to the desingularization of (variational) criticality and its consequences to the asymptotic analysis of (nonsmooth) dynamical systems.

Joint work with The talk is based on several works obtained in collaboration with J. Bolte (Université Toulouse 1, France), D. Drusvyatskiy (University of Washington, USA) and A. S. Lewis (Cornell University, USA).

A6 - December 11, 17:30 – 18:00

ELEMENTARY RECURSIVE DEGREE BOUNDS FOR POSITIVSTELLENSATZ, HILBERT 17TH
PROBLEM AND REAL NULLSTELLENSATZ (PART I)

Daniel Perrucci

Universidad de Buenos Aires, Argentina
perrucci@dm.uba.ar

Hilbert 17th problem is to express a non-negative polynomial as a sum of squares of rational functions. The original proof by Artin is non-constructive and gives no information on the degree bounds.

A more general problem is to give an identity which certifies the unrealizability of a system of polynomial equations and inequalities. The existence of such an identity is guaranteed by the Positivstellensatz. Hilbert 17th problem, as well as Real Nullstellensatz follow easily from such identities.

In these two talks, we explain our new constructive proof which provides elementary recursive bounds for the Positivstellensatz and Hilbert 17 problem, namely a tower of five levels of exponentials.

Joint work with Henri Lombardi (Université de Franche-Comté, France) and Marie-Françoise Roy (Université de Rennes 1, France).

A6 - December 11, 18:00 – 18:30

ELEMENTARY RECURSIVE DEGREE BOUNDS FOR POSITIVSTELLENSATZ, HILBERT 17TH
PROBLEM AND REAL NULLSTELLENSATZ (PART II)

Marie-Françoise Roy

Université de Rennes 1, France
marie-francoise.roy@univ-rennes1.fr

Hilbert 17th problem is to express a non-negative polynomial as a sum of squares of rational functions. The original proof by Artin is non-constructive and gives no information on the degree bounds.

A more general problem is to give an identity which certifies the unrealizability of a system of polynomial equations and inequalities. The existence of such an identity is guaranteed by the Positivstellensatz. Hilbert 17th problem, as well as Real Nullstellensatz follow easily from such identities.

In these two talks, we explain our new constructive proof which provides elementary recursive bounds for the Positivstellensatz and Hilbert 17 problem, namely a tower of five levels of exponentials.

Joint work with Henri Lombardi (Université de Franche-Comté, France) and Daniel Perrucci (Universidad de Buenos Aires, Argentina).

A6 - December 11, 18:30 – 19:00

TOWARDS A BROADER VIEW OF THEORY OF COMPUTING – PART 1

Narendra Karmarkar

Indian Institute of Technology, Bombay, India
narendrakarmarkar@yahoo.com

Beginning with the projectively invariant method for linear programming, interior point methods have led to powerful algorithms for many difficult computing problems, in combinatorial optimization, logic, number theory and non-convex optimization. Algorithms for convex optimization benefitted from many

pre-established ideas from classical mathematics, but non-convex problems require new concepts. This three part series outlines some of these concepts— computational models based on the concept of the continuum, algorithms invariant w.r.t. projective , bi-rational , and bi-holomorphic transformations on co-ordinate representation, extended proof systems for more efficient certificates of optimality, extensions of Grassmann’s extension theory, efficient evaluation methods for the effect of exponential number of constraints , theory of connected sets based on graded connectivity, theory of curved spaces adapted to the problem data, and concept of “ relatively” algebraic sets in curved space.

Models of Computation provide mathematical abstractions of basic data objects and operations on them available as building blocks. This effectively decouples design of algorithms for complex tasks from lower level details of how the underlying hardware implements the building blocks. The Turing machine model uses strings of 0’s and 1’s and finite state machines. Careful study of the work of early pioneers – Turing, Von Neumann and Godel – shows that they were acutely aware of the limitations of this model for comprehensive understanding of the fundamental aspects of computation. BSS model uses real or complex numbers as data objects and algebraic operations (including comparisons in real case). This is more natural for many algorithms in numerical analysis. Various computing models can be organized in a similar way as Cantor had organized infinite sets—by cardinal number of the set of all possible machines and data objects in the model. Staying within the same cardinal number, a more powerful approach is to use further extension, e.g real analytic functions or algebraic closure of meromorphic functions over suitable domains. Operations include algebraic as well as analytic operations. i.e. integration and differentiation are regarded as binary operations. (specification of the contour of integration is one of the input operands) All such models are collectively referred to as continuum computing. Time permitting, more topics from the list above will be covered in the first part.

A6 - December 12, 14:30 – 15:00

DE RHAM COHOMOLOGY AND ORDINARY DIFFERENTIAL EQUATIONS

Peter Scheiblechner

Lucerne University of Applied Sciences and Arts, Switzerland
peter.scheiblechner@hslu.ch

We describe an EXPSPACE-algorithm for computing the de Rham cohomology of the complement of an affine hypersurface over the complex numbers. The best previously known algorithm for this problem (cylindrical algebraic decomposition) needs double exponential time. Our algorithm follows the lines of a proof of Monsky for the finite dimensionality of the de Rham cohomology. It reduces the computation of the cohomology to certain systems of ordinary differential equations with Laurent polynomial coefficients. We study the complexity of the solutions of such systems.

A6 - December 12, 15:00 – 15:30

CAN EVERYTHING BE COMPUTED? - ON THE SOLVABILITY COMPLEXITY INDEX AND TOWERS OF ALGORITHMS

Anders Hansen

University of Cambridge, United Kingdom
ach70@cam.ac.uk

This talk addresses some of the fundamental barriers in the theory of computations. Many computational problems can be solved as follows: a sequence of approximations is created by an algorithm, and the

solution to the problem is the limit of this sequence (think about computing eigenvalues of a matrix for example). However, as we demonstrate, for several basic problems in computations (computing spectra of infinite dimensional operators, solutions to linear equations or roots of polynomials using rational maps) such a procedure based on one limit is impossible. Yet, one can compute solutions to these problems, but only by using several limits. This may come as a surprise, however, this touches onto the boundaries of computational mathematics. To analyze this phenomenon we use the Solvability Complexity Index (SCI). The SCI is the smallest number of limits needed in order to compute a desired quantity. In several cases (spectral problems, inverse problems) we provide sharp results on the SCI, thus we establish the absolute barriers for what can be achieved computationally. For example, we show that the SCI of spectra of self-adjoint infinite matrices is equal to two, thus providing the first algorithms to compute such spectra in two limits. Moreover, we establish barriers on error control. We prove that no algorithm can provide error control on the computational spectral problem or solutions to infinite-dimensional linear systems. In particular, one can get arbitrarily close to the solution, but never knowing when one is “epsilon” away. In addition, we provide bounds for the SCI of spectra of classes of Schrodinger operators, thus we affirmatively answer the long standing question on whether or not these spectra can actually be computed. Finally, we show how the SCI provides a natural framework for understanding barriers in computations. In particular, we demonstrate how the impossibility result of McMullen on polynomial root finding with rational maps in one limit, and the framework of Doyle and McMullen on solving the quintic in several limits, can be put in the SCI framework.

Joint work with Jonathan Ben-Artzi (University of Cambridge), Olavi Nevanlinna (Aalto University), Markus Seidel (TU Chemnitz).

A6 - December 12, 15:35 – 16:25

PROBABILISTICALLY CHECKABLE PROOFS OVER THE REALS

Klaus Meer

Brandenburg Technical University Cottbus - Senftenberg, Germany
 meer@informatik.tu-cottbus.de

One fruitful source of interesting problems in structural complexity theory over the reals since its introduction by Blum, Shub, and Smale in 1989 has been the investigation of major theorems known in classical (Turing) complexity within the real number framework. Prominent examples are the P versus NP question, decidability algorithms for problems in NP over the reals, and the theorems by Ladner and Toda, to mention a few only.

A cornerstone in Turing complexity theory is the PCP theorem shown in the early 1990’s by Arora et al. It gives an alternative characterization of the complexity class NP via so-called probabilistically checkable proofs. Roughly speaking, it shows that a verification algorithm for instances of problems in NP can be designed such that a false verification proof can be detected with high probability by reading constantly many proof bits only. The theorem has shown huge impact on approximation problems as well.

It is thus natural to ask whether a similar characterization holds for the class $NP_{\mathbb{R}}$ of problems in NP over the reals. This boils down to the question whether there is a (randomized) procedure that verifies a solvability proof of a polynomial system over the reals by only inspecting a constant number of real components in the proof. Obviously, the natural $NP_{\mathbb{R}}$ -verification proof that takes a zero and just plugs it into the system fails.

In the talk we shall report on techniques and results that we have been working on during the last couple of years in order to design real number PCPs. We explain the role of property testing and shall outline the proof of the corresponding PCP theorem both in the real and complex number BSS model. A focus

will be on highlighting the differences (and non-differences) to the existing proofs of the classical PCP theorem.

Joint work with Martijn Baartse (Brandenburg Technical University Cottbus - Senftenberg, Germany).

A6 - December 12, 17:00 – 17:30

GEOMETRIC COMPLEXITY THEORY, TENSOR RANK, AND REPRESENTATION THEORY

Christian Ikenmeyer

Texas A&M University, USA
ciken@math.tamu.edu

Mulmuley and Sohoni conjectured that the permanent vs determinant problem can be resolved using explicit so-called representation theoretic occurrence obstructions. It is still unknown whether these objects exist or not, even for small examples. We show that in the simpler (but still highly interesting) setting of matrix multiplication these obstructions indeed exist! We prove the lower bound $R(M_m) \geq \frac{3}{2}m^2 - 2$ on the border rank of $m \times m$ matrix multiplication by exhibiting explicit representation theoretic occurrence obstructions. While this bound is weaker than the one recently obtained by Landsberg and Ottaviani, these are the first significant lower bounds obtained within the GCT program. Behind the proof is basically Schur-Weyl duality and an explicit description of highest weight vectors in terms of combinatorial objects.

Joint work with Peter Bürgisser (Technische Universität Berlin, Germany).

A6 - December 12, 17:30 – 18:00

ON THE INTERSECTION OF A SPARSE CURVE AND A LOW-DEGREE CURVE: A POLYNOMIAL VERSION OF THE LOST THEOREM

Pascal Koiran

Ecole Normale Supérieure de Lyon, France
pascal.koiran@ens-lyon.fr

Consider a system of two polynomial equations in two variables:

$$F(X, Y) = G(X, Y) = 0$$

where $F \in \mathbb{R}[X, Y]$ has degree $d \geq 1$ and $G \in \mathbb{R}[X, Y]$ has t monomials. We show that the system has only $O(d^3t + d^2t^3)$ real solutions when it has a finite number of real solutions. This is the first polynomial bound for this problem. In particular, the bounds coming from the theory of fewnomials are exponential in t , and count only nondegenerate solutions. More generally, we show that if the set of solutions is infinite, it still has at most $O(d^3t + d^2t^3)$ connected components.

By contrast, the following question seems to be open: if F and G have at most t monomials, is the number of (nondegenerate) solutions polynomial in t ?

The authors' interest for these problems was sparked by connections between lower bounds in algebraic complexity theory and upper bounds on the number of real roots of "sparse like" polynomials.

Joint work with Natacha Portier and Sébastien Tavenas.

A6 - December 12, 18:00 – 18:30

A POLYNOMIAL HOMOTOPY RANDOM WALK

Anton Leykin

Georgia Tech, USA

leykin@math.gatech.edu

Given a one parameter family of polynomial systems with complex coefficients, we develop a new way of tracking an initial system-solution pair to a solution of the target system. While the theoretical complexity is believed to be, at best, the same as for traditional approaches, there are practical advantages to this method in certain scenarios. (Work in progress.)

A6 - December 13, 14:30 – 15:00

UNIVERSAL COMPONENTS OF RANDOM ALGEBRAIC SETS

Damien Gayet

Institut Fourier, Grenoble 1, France

gayetd@ujf-grenoble.fr

I will explain that any compact hypersurface S of R^n appears with a positive probability c_S as a component of a random algebraic hypersurface of high degree d , with c_S not depending on d .

Joint work with Jean-Yves Welschinger (Institut Camille Jordan, Lyon 1, France).

A6 - December 13, 15:00 – 15:30

ON THE NUMBER OF ZEROS OF E -POLYNOMIALS

Gabriela Jeronimo

Universidad de Buenos Aires - CONICET, Argentina

jeronimo@dm.uba.ar

An E -polynomial in a single variable with integer coefficients is a real function of the form $P(x, e^{h(x)})$, where $P(X, Y) \in \mathbb{Z}[X, Y]$ and $h \in \mathbb{Z}[X]$. These functions form a particular subclass of the so-called Pfaffian functions introduced by Khovanskii in the 70's. As proved by Vorobjov in 1992, the consistency problem for (multivariate) E -polynomials is algorithmically decidable.

We will present an algorithm for the computation of the number of zeros of an E -polynomial in \mathbb{R} and in an interval of \mathbb{R} . Our algorithm is inspired in the well-known Sturm's Theorem for real univariate polynomials. It relies on the construction, from the polynomials P and h , of adequate sequences of E -polynomials and the sign determination of their evaluation at algebraic real numbers. We prove that the number of real zeros of $P(x, e^{h(x)})$ can be computed from the number of sign changes of these sequences evaluated at finitely many points that are obtained throughout the construction. In order to determine sign changes, we also develop an algorithmic procedure to compute the sign of an E -polynomial evaluated at an algebraic real number given by its Thom encoding.

Joint work with María Laura Barbagallo (Universidad de Buenos Aires - CONICET), Juan Sabia (Universidad de Buenos Aires - CONICET).

A6 - December 13, 15:30 – 16:00

QUIZ GAMES: A MODEL FOR INFORMATION HIDING

Luis M. Pardo

University of Cantabria, Spain

luis.m.pardo@gmail.com

In this talk I introduce a model for information hiding in Elimination Theory. The model we call Quiz Game is an interactive protocol based on a single round two-players game, admitting exact and approximate models. The model extends existing models like robust algorithms, universal algorithms or software engineering models in Elimination Theory, shown in former outcomes of the same current of thought. The main outcome here is to show that a player with a winning strategy for Elimination Problems requires exponential size abstract data types and, hence, any winning strategy cannot be efficient. Similar results are shown for the evaluation of characteristic polynomials, interpolation of straight-line programs and elementary arithmetic neural networks. This is ongoing research written with B. Bank, J. Heintz, G. Matera and A. Rojas-Paredes.

A6 - December 13, 16:00 – 16:30

COUNTING THE NUMBER OF COMPONENTS OF RANDOM REAL HYPERSURFACES

Antonio Lerario

Institut Camille Jordan, Lyon, France

anto.lerario@gmail.com

To determine the average number of real zeroes of a univariate polynomial whose coefficients are random variables is a classical and well studied problem. A natural way to generalize it is to ask for the average number of connected components of the zero set of a random polynomial in several variables. This approach is much influenced by a random approach to Hilbert's Sixteenth Problem, to study the number and the arrangement in the projective space of the components of a real algebraic hypersurface.

The answer to the above question (both in the univariate and the multivariable case) strongly depends on the choice of the probability distribution.

In this talk I will show that, if the probability distribution is Gaussian and has no preferred points or directions in the projective space, the case of several variables can be reduced to the classical univariate problem. More precisely, the number of connected components of a random hypersurface in $\mathbb{R}P^n$ of degree d has the same order of the number of points of intersection of this hypersurface with a fixed projective line, raised to the n -th power.

Joint work with Yan V. Fyodorov (School of Mathematical Sciences, Queen Mary University of London) and Erik Lundberg (Department of Mathematics, Florida Atlantic University).

A6 - December 13, 17:00 – 17:30

ON THE COMPUTATION OF ROADMAPS OF REAL ALGEBRAIC SETS

Eric Schost

Western University, Canada

eschost@uwo.ca

We consider the question of constructing roadmaps of real algebraic sets, which was introduced by Canny to answer connectivity questions and solve motion planning problems. Canny's algorithm is recursive, but decreases the dimension only by one through each recursive call.

In this talk, we present a divide-and-conquer version of Canny's algorithm, where the dimension is halved through each recursive call. The input is a compact complete intersection V given by polynomials of degree D in n variables; we also have to assume that V has a finite number of singular points.

We also mention results of a preliminary implementation, and may indicate how the calculation of points on some Thom-Boardman strata could explain some of these results.

Joint work with Mohab Safey El Din (Universite Pierre et Marie Curie (Paris 6), France).

A6 - December 13, 17:30 – 18:00

THE BETTI NUMBERS OF AN INTERSECTION OF RANDOM QUADRICS

Erik Lundberg

Florida Atlantic University, USA
elundber@fau.edu

Let X be an intersection of k quadrics chosen at random from the so-called Kostlan ensemble. As the number of variables increases, we study the asymptotics of each Betti number of X and show that the expected i th Betti number is asymptotically one. In particular, an intersection of quadrics is asymptotically connected on average. In the case of an intersection of $k = 2$ quadrics, we give additional detail on the sum of all Betti numbers, providing an asymptotic with two orders of precision. The proofs apply the Agrachev-Lerario spectral sequence from Algebraic Topology combined with results from Random Matrix Theory. The case of three quadrics leads to considering a new model for random curves based on determinantal representations.

Joint work with Antonio Lerario (Lyon 1, France).
