Report from Dagstuhl Seminar 15242

Complexity of Symbolic and Numerical Problems

Edited by

Peter Bürgisser[1], Felipe Cucker[2], Marek Karpinski[3], and Nicolai Vorobjov[4]

1 **TU Berlin, DE**
2 **City University – Hong Kong, HK,** `macucker@cityu.edu.hk`
3 **Universität Bonn, DE,** `marek@cs.uni-bonn.de`
4 **University of Bath, GB,** `nnv@cs.bath.ac.uk`

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 15242 "Complexity of Symbolic and Numerical Problems".

Seminar June 7–12, 2015 – http://www.dagstuhl.de/15242
1998 ACM Subject Classification F.2.1 Numerical Algorithms and Problems, F.2.2 Nonnumerical Algorithms and Problems.
Keywords and phrases Symbolic computation, Algorithms in real algebraic geometry, Complexity lower bounds, Geometry of numerical algorithms
Digital Object Identifier 10.4230/DagRep.5.6.28

1 Executive Summary

Peter Bürgisser
Felipe Cucker
Marek Karpinski
Nicolai Vorobjov

The seminar was dedicated to Prof. Dima Grigoriev on the occasion of his 60th birthday. Its aim was to discuss modern trends in computational real algebraic geometry, in particular, areas related to solving real algebraic and analytic equations and inequalities. Very recent new developments in the analysis of these questions from the point of view of *tropical mathematics* were also presented.

Historically there were two strands in the computational approach to polynomial systems' solving. One is the tradition of numerical analysis, a classical achievement of which is the *Newton's method*. Various other approximation algorithms were developed since then, some based on the idea of a *homotopy*. Numerical analysis did not bother to introduce formal models of computations (and hence computational complexity considerations) but developed refined methods of estimations of convergency rates. Another tradition emerged from algebra, particularly in classical works of Cayley, Sylvester and Macaulay. Algebraic results concerning *real* solutions go further back to the Descartes' rule and Sturm sequences. An important contribution to the subject from logic was Tarski's constructive quantifier elimination procedures for algebraically closed and real closed fields. The computations considered in this tradition are exact, under modern terminology – "symbolic". They

naturally fit into standard models of computation (Turing Machines, straight-line programs, computation trees) thus lending themselves to complexity analysis.

Until 1990s these two strands developed largely independently. One of the important unifying ideas became the concept of a *real numbers* (or *BSS*) machine suggested by Blum, Shub and Smale which can be considered as a model of computation for the numerical analysis. This idea led to Smale's 9th and 17th problems, which became an inspiration for many researchers in the field.

The seminar considered a wide set of questions related to the current state of the symbolic and numeric approaches to algorithmic problems of real algebraic and analytic geometry, also from the novel perspective of tropical and max/plus mathematics.

2 Table of Contents

3 Overview of Talks

In this section we give a very coarse general outline of the results presented at the seminar. The reader should consult the *Abstracts* section for a more precise description of the talks.

One of the conceptually most simple and computationally efficient methods for deciding consistency of systems of polynomial equations over algebraically closed fields is based on *Effective Hilbert's Nullstellensatz* – the theorem known since late 1980s. Over real closed fields, where polynomial inequalities make sense, the analogy of the classical Hilbert's Nillstellensatz is *Positivstellensatz* (in different versions). This seminar was one of the first conferences where the new breakthrough result was announced: an elementary recursive bound for Effective Positivstellensatz and Hilbert 17-th problem, proved by H. Lombardi, D. Perrucci, and M.-F. Roy.

In tropical mathematics, the research of algorithmic and complexity issues had started only very recently, and mostly in linear algebra. One of the first complexity results in polynomial algebra, *Tropical Effective Nullstellensatz*, was reported at the seminar by V. Podolskii (joint work with D. Grigoriev). This remarkable achievement starts a new chapter in symbolic computer algebra. In the talk of A. Weber, complexity aspects of tropical algebra were applied to bio-chemical reaction networks.

In complexity theory, the Graph Isomorphism problem is one of the most exciting since it is not known to be NP-complete or belong to P. On the other hand, the problem is polynomially equivalent to finding the automorphism group of a colored graph. In the talk of I. Ponomarenko, for the important particular case of the latter problem, the Cartan association scheme, an algorithm with polynomial complexity was presented.

Talks of F. Cucker, D. Amelunxen, and P. Bürgisser were dedicated to the latest advances in complexity theory of numerical algorithms, foundations of which were developed in the recent monograph "Condition" by Bürgisser and Cucker. Cucker presented a theory of complexity for numerical computations that takes into account the condition of the input data and allows for roundoff in the computations. Amelunxen proposed a new model for probabilistic analysis of condition numbers which, when applied to the convex feasibility problem, yields a dramatic improvement in complexity (joint work with M. Lotz). Bürgisser presented a proof of the condition number theorem, characterizing the *condition* of computing a point in the intersection of a fixed complex projective variety with an input linear subspace of the complement dimension.

A number of talks described recent breakthroughs concerning problems in classical complexity theory. D. Grigoriev applied a technique of cluster algebras to close a long-standing problem on the comparative complexity power between all possible subsets of operations $+$, $-$, $\times$, $/$ in arithmetic circuits. This is done via computing Schur functions (joint work with S. Fomin and G. Koshevoy). É. Shost gave in his talk an alternative algorithm for computing Schur functions. N. Vorobjov presented complexity lower bounds for testing membership in semi-algebraic sets on algebraic computation trees and arithmetic networks (joint work with A. Gabrielov). Using recent advances in o-minimal topology the classical lower bounds of Yao and Montaña-Morais-Pardo were expanded to singular homology on arbitrary semi-algebraic sets. Within the theme of classical complexity, K. Meer suggested a new, algebraic, proof of the real number PCP (probabilistically checkable proof) theorem (joint work with M. Baartse). This result is an exact match with the main motive of the seminar: interplay between symbolic and numerical approaches to computation.

A group of seminar talks discussed aspects of computer algebra. J. Davenport reported on practical improvements in Cylindrical Algebraic Decomposition algorithm (a subroutine

extensively used in, e.g., Maple), in the presence of equational constraints. S. Basu presented a theory of symmetric groups acting on symmetric real algebraic varieties, semi-algebraic sets, and symmetric complex varieties in affine and projective spaces, defined by polynomials of fixed degrees. He gave polynomial bounds on the number of irreducible representations of such groups, as well as their multiplicities (joint work with C. Riener). P. Koiran explained a version of a fewnomial theorem. It turns out that in the case of two polynomial equations in two variables, when one has a degree $d \geq 1$ and another t monomials, the number of real solutions is polynomial in d and t when this number is finite. This result is in sharp contrast with the famous Khovanskii's general bound, which is exponential in t. M. Safey El Din presented a new algorithm for computing roadmaps in smooth algebraic sets, having the lowest complexity achieved so far (joint work with É. Schost). A classical topic in computer algebra was re-run by E. Kaltofen, who reproduced his 1987 talk on fast multiplication of polynomials over arbitrary rings with various modern witty comments.

The seminar featured a number of talks on a broad subject of convex geometry which are related to both symbolic and numerical computing. D. Pasechnik considered the problem of reconstructing a measure in $\mathbb{R}^d$ from a truncated multi-sequence of its moments, in an important particular case of a measure with piecewise-polynomial density supported on a compact polyhedron. He showed that this problem can be solved exactly (joint work with N. Gravin, and B. and M. Shapiro). M. Lotz discussed various applications of spherical integral geometry, in particular the complexity theory of conic optimization and convex optimization approaches to solving underdetermined systems of equations. T. Theobald revisited a classical problem of the complexity of deciding containment of one polyhedron in another, where polyhedra can be defined either by linear inequalities or as convex hulls, in any combination. The novel approach uses sums of squares technique (joint work with K. Kellner).

Modern cryptography was represented by the talk of V. Spilrain. He explained a revolutionary approach to building public key cryptosystems, based on laws of classical physics, and not using any trapdoor functions (joint work with D. Grigoriev).

A. O. Slissenko presented a novel view on the work of an algorithm as a process of the decreasing uncertainty (entropy) about the output. The complexity aspect of this approach requires understanding of what is the speed of this decreasing. A technique is suggested which allows to develop an adequate definition.

The talk by E. Hirsch was devoted to a major conjecture in proof complexity: the existence of an algorithm, called acceptor, that is optimal on all propositional tautologies. It was claimed that in the presence of errors such optimal algorithm exists (joint with D. Itsykson, I. Monakhov, A. Smal).

4 Abstracts of talks

4.1 An elementary recursive bound for effective Positivstellensatz and Hilbert 17-th problem

Marie-Françoise Roy (University of Rennes, FR)

Joint work of Marie-Françoise Roy, Henri Lombardi, Daniel Perrucci

We prove the first elementary recursive bounds in the degrees for Positivstellensatz and Hilbert 17-th problem, which is the expression of a nonnegative polynomial as a sum of squares of rational functions. We obtain a tower of five exponentials. A precise bound in terms of the number and degree of the polynomials and their number of variables is provided. (See http://arxiv.org/abs/1404.2338v2.)

4.2 Tropical Effective Nullstellensatz

Vladimir Podolskii (Steklov Institute – Moscow, RU)

Joint work of Vladimir Podolskii, Dima Grigoriev

A tropical (or min-plus) semiring is a set real numbers, possibly with infinity, endowed with two operations: tropical addition, which is just usual minimum operation, and tropical multiplication, which is usual addition. Tropical polynomials can be defined analogously to classical polynomials. In tropical algebra, a tuple $\mathbf{x}$ is a solution to a multivariate polynomial $\min(g_1(\mathbf{x}), g_2(\mathbf{x}), \ldots, g_k(\mathbf{x}))$, where $g_i(\mathbf{x})$'s are tropical monomials, if the minimum is attained at least twice. If we consider a convex piece-wise linear function given by a tropical polynomials, then roots correspond to non-smoothness points of the function.

In this talk we present a tropical effective analog of Hilbert's Nullstellensatz.

4.3 Recognizing the Cartan association schemes in polynomial time

Ilia Ponomarenko (Steklov Institute – St. Petersburg, RU)

It is well known that the Graph Isomorphism Problem is polynomially equivalent to finding the automorphism group of a colored graph. In the present talk, we deal with a special case of the latter problem. Namely, the Cartan association scheme can be thought of as the complete colored graph the color classes of which are the orbits of a finite group with BN-pair that acts on the cosets of the Cartan subgroup $B \cap N$. We show that the following problem can be solved in a polynomial time (in the number of vertices): given a colored complete graph check whether it is a Cartan scheme associated with a simple group and (if so) find the automorphism group of the graph.

4.4 Empiric investigations of some seemingly slowly growing complexity parameters of bio-chemical reaction networks

Andreas Weber (Universität Bonn, DE)

Joint work of Andreas Weber, Dima Grigoriev, Ovidiu Radulescu, Satya Swarup Samal

Bio-chemical reaction networks are bi-partitite graphs involving the reacting species and the reactions as vertices. These can range from a few for so called *network motifs* up to several thousands (e.g., for networks reconstructing yeast metabolism or human metabolism). Assuming well-mixing and mass action kinetics, the dynamics of the networks is given by a system of ordinary differential equations with polynomial vector fields. Whereas a priori only little special structure is known to reduce the complexity of several computational tasks on the given systems, it has recently been shown that the tree width of the networks is growing slowly (and even being smaller than 6 for most networks). In this talk we will focus on computing tropical equilibrations, which are important for several purposes, e.g. for model reduction, but is an NP-complete task in general. Performing computations on the BIOMODELS database we found that the number of maximal solution polytopes is much smaller than had to be expected.

4.5 A Theory of Complexity, Condition, and Roundoff

Felipe Cucker (City University – Hong Kong, HK)

We develop a theory of complexity for numerical computations that takes into account the condition of the input data and allows for roundoff in the computations. We follow the lines of the theory developed by Blum, Shub, and Smale for computations over $\mathbb{R}$ (which in turn followed those of the classical, discrete, complexity theory as laid down by Cook, Karp, and Levin among others). In particular, we focus on complexity classes of decision problems and paramount among them, on appropriate versions of the classes P, NP and EXP of polynomial, nondeterministic polynomial, and exponential time, respectively. We prove some basic relationships between these complexity classes and exhibit natural NP-complete problems.

4.6 On a blindspot in probabilistic analysis of condition numbers

Dennis Amelunxen (City University – Hong Kong, HK)

Joint work of Dennis Amelunxen, Martin Lotz

The common practice in the probabilistic analysis of condition numbers suffers from a strange imbalance in the model, which seems to have gone unnoticed so far. On the one hand it is emphasized that the use of condition numbers takes into account real-world limitations of numerical computations such as the effects of floating-point arithmetics, while on the other

hand an overly strict mathematical model is used, which prevents the inclusion of important effects in high-dimensional geometry that are loosely summarized by the term "concentration of measure".

We propose a small but decisive change in the model used in the probabilistic analysis, which broadly consists of replacing the nullset of ill-posed inputs by an exponentially small set. While this change is easily accepted from an applications point of view, the resulting change in the probabilistic behavior of the condition number can be dramatic. Indeed, in the case of the convex feasibility problem the expectation of Renegar's condition number (not its logarithm!) has constant "weak average-case complexity", as opposed to infinity, which is the answer in the classical form and which is in stark contrast to what is being observed in practice. The argument for this result is surprisingly simple.

4.7 Subtraction-free computations and cluster algebras

Dima Grigoriev (Lille I University, FR)

Joint work of Dima Grigoriev, S. Fomin, G. Koshevoy

Using cluster transformations we design subtraction-free algorithms for computing Schur polynomials and for generating spanning trees and arborescences polynomials. The latter provides an exponential complexity gap between circuits admitting arithmetic operations $+, \times, /$ versus $+, \times$. In addition, we establish an exponential complexity gap between circuits admitting $+, -, \times, /$ versus $+, \times, /$. Together with V. Strassen's result on "Vermeidung von Divisionen" this closes a long-standing problem on comparative complexity power between all possible subsets of operations $+, -, \times, /$.

4.8 On Entropic Convergence of Algorithms

Anatol Slissenko (Université Paris-Est Créteil, FR)

This talk presents an attempt to find an information based view on the work of an algorithm. Unfortunately, there is no mathematical notion of information that adequately reflects our intuition. The only related notion, as far as I know, is that of entropy – that is a measure of uncertainty.

It is intuitively clear that an algorithm, while computing a function, diminishes the uncertainty of its knowledge about the result. The question is how to estimate quantitatively the speed of this decreasing of the uncertainty. In order to define entropy we introduce a probabilistic measure on the domain of deterministic algorithm on the basis of principle of Maximal Uncertainty: the uncertainty about the result is maximal if all the results are equiprobable. The measure is over inputs of a fixed length (for better intuition one may think that this set is of exponential size). It depends only on the graph of the computed function, not on the algorithm. Denote by f the function computed by an algorithm $\mathfrak{A}$, and by $\boldsymbol{dm}(f)$ and $\boldsymbol{rn}(f)$ the set of its inputs of a fixed size and respectively its range $f(\boldsymbol{dm}(f))$. The measure is $\boldsymbol{P}(f^{-1}(v)) = \frac{1}{|\boldsymbol{rn}(f)|}$, and it is uniform on $f^{-1}(v)$, $v \in \boldsymbol{rn}(f)$.

After that, and this is the next conceptual difficulty, we introduce a mapping of events of the algorithm under study, into partitions of subsets of $\boldsymbol{dm}(f)$. The work of $\mathfrak{A}$ is treated as the set of its traces. A trace $\boldsymbol{tr}(X)$ of $\mathfrak{A}$ for an element $X \in \boldsymbol{dm}(f)$ is a sequence of commands executed by $\mathfrak{A}$ for input X (plus the initial state that we do not make explicit), each such execution being an update (assignment) or a guard (evaluated as true); these are *events*, and $\boldsymbol{tr}(X,t)$ is the event at an instant t.

The mapping of events into partitions is based on some notion of similarity $\sim$ of events (which is assumed to be an equivalence). First, an event $E = \boldsymbol{tr}(X,t)$ is associated with a set $\widehat{E}$ of inputs X' such that $\boldsymbol{tr}(X,t) \sim \boldsymbol{tr}(X',t')$ for some t'. This set defines its ordered partition $\pi(E)$ into intersection of $\widehat{E}$ with $f^{-1}(v)$ for a fixed order of $\boldsymbol{rn}(f)$. For such a partition its entropy conditioned by $\widehat{E}$ is denoted $\mathcal{D}(E)$.

A metric function can be defined on $\pi(E)$. Not all events are informative, e.g., the loop counter gives nothing. Modulo this remark, sequences $\big(\mathcal{D}(\boldsymbol{tr}(X,t))\big)_t$, $X \in \boldsymbol{dm}(f)$, and the space $\mathfrak{R}(t) = \{\pi(\boldsymbol{tr}(X,\tau)) : X \in \boldsymbol{dm}(f) \wedge \tau \geq t\}$ give descriptions of entropic convergence of $\mathfrak{A}$.

4.9 Nature-based information security

Vladimir Shpilrain (City University of New York, US)

Joint work of Vladimir Shpilrain, Dima Grigoriev

We use various laws of classical physics to offer several solutions of Yao's millionaires' problem without using any one-way functions. We also describe informationally secure public key encryption protocols, i.e., protocols secure against passive computationally unbounded adversary. This introduces a new paradigm of decoy-based cryptography, as opposed to "traditional" complexity-based cryptography.

4.10 Equational Constraints and Cylindrical Algebraic Decomposition

James H. Davenport (University of Bath, GB)

Quantifier Elimination by Cylindrical Algebraic Decomposition is easier if there is a global equational constraint $f = 0 \wedge \cdots$. We have recently extended this to local equational constraints (R.J. Bradford, J.H. Davenport, M. England, S. McCallum, and D.J. Wilson, Proceedings ISSAC 2013, 125–132). We present this, and work in press (`arXiv1401.0645; 1501.04466`) on multiple equational constraints, and where the local equational constraints do not give a global constraint. This last is particularly useful for motion planning and branch cut applications. See http://staff.bath.ac.uk/masjhd/Slides/JHDatDagstuhlJune2015.pdf.

4.11 Condition of intersecting a fixed projective variety with a given linear subspace

Peter Bürgisser (TU Berlin, DE)

Let $Z \subseteq \mathbb{P}^n$ be a fixed complex projective variety of dimension m and put $s := n - m$. We define the *condition* $\kappa(L, z)$ of computing a point of intersection $z \in Z \cap L$ for an input $L \in \mathrm{Grass}(\mathbb{P}^n, s)$ in the Grassmann manifold of s-dimensional linear subspaces as the operator norm of the (locally defined) solution map $L \mapsto z$ (if the intersection is transversal and z is smooth). We characterize $\kappa(L, z)$ in terms of the minimal principal angle between the tangent spaces $T_z Z$ and $T_z L$, and use this to prove a *condition number theorem* that characterizes $\kappa(L, z)$ as the inverse distance of L to a local Schubert variety of ill-posedness. Hence a probabilistic analysis of the maximum condition number $\kappa(L) := \max\{\kappa(L, z) \mid z \in Z \cap L\}$ is reduced to bounding the volume of the ε-tube around the hypersurface $\Sigma \subseteq \mathrm{Grass}(\mathbb{P}^n, s)$ of ill-posed subspaces touching Z. As a first step towards this goal, we prove that $\mathrm{vol}(\Sigma)/\mathrm{vol}(\mathrm{Grass}(\mathbb{P}^n, s)) = \deg(\Sigma)(s+1)(n-s)/\pi$.

4.12 An algebraic proof of the real number PCP theorem

Klaus Meer (BTU Cottbus, DE)

Joint work of Klaus Meer, M. Baartse

The PCP theorem is a major achievement in theoretical computer science in the last two decades. There exist two intrinsically different proofs of it. The original one by Arora et al. being algebraic in nature, and a more recent one by Dinur based on graph theoretic techniques.

We are interested in PCP theorems for the real number model of computation introduced by Blum, Shub, and Smale. In earlier work we could prove the real number PCP theorem to hold along the lines of Dinur's proof. In this talk we report on an algebraic proof of the theorem. It is close in structure to the original one by Arora et al., but needs additional efforts to deal with several problems arising on the way.

4.13 On the isotypic decomposition of cohomology modules of symmetric semi-algebraic sets: polynomial bounds on multiplicities

Saugata Basu (Purdue University – West Lafayette, US)

Joint work of Saugata Basu, Cordian Riener

We consider symmetric (as well as multi-symmetric) real algebraic varieties and semi-algebraic sets, as well as symmetric complex varieties in affine and projective spaces, defined by polynomials of fixed degrees. We give polynomial (in the dimension of the ambient space)

bounds on the number of irreducible representations of the symmetric group which acts on these sets, as well as their multiplicities, appearing in the isotypic decomposition of their cohomology modules with coefficients in a field of characteristic 0. We also give some applications of our methods in proving lower bounds on the degrees of defining polynomials of certain symmetric semi-algebraic sets, as well as improved bounds on the Betti numbers of the images under projections of (not necessarily symmetric) bounded real algebraic sets.

Finally, we conjecture that the multiplicities of the irreducible representations of the symmetric group in the cohomology modules of symmetric semi-algebraic sets defined by polynomials of fixed degrees are computable with polynomial complexity, which would imply that the Betti numbers of such sets are also computable with polynomial complexity. This is in contrast with general semi-algebraic sets, for which this problem is provably hard (#**P**-hard).

4.14 Rational moment generating functions and polyhedra

Dmitrii V. Pasechnik (University of Oxford, GB)

Joint work of Dmitrii V. Pasechnik, Nick Gravin, Boris Shapiro, Michael Shapiro

The problem of reconstructing a measure in $\mathbb{R}^d$ from a (truncated) multi-sequence of its moments has important applications, and is in general very hard to solve. We concentrate on a natural case of a measure m with piecewise-polynomial density supported on a compact polyhedron P, and show that such problems can be solved exactly, due to existence of a natural integral transform of the measure (known as Fantappie transformation), which is a rational function $F_m(u)$.

The denominator of $F_m(u)$ is the product of linear functions of the form $1 - \langle u, v\rangle$, with v belonging to certain finite multiset $V(P)$. $F_m(u)$ is closely related to a more well-known Laplace transform $L_m(u)$ of a related "conified" measure arising in the theory of hyperplane arrangements. It is an interesting problem to reconstruct F_m (or L_m) from the noisy data; this would entail approximate Pade approximation and/or factoring into linear terms.

There are interesting applications of L_m to compact (not necessarily convex) polyhedra P. Let $I(P)$ be the indicator function of P. Then $I(P)$ can be decomposed (up to a measure 0 subset) as a sum, with $+1$ or -1 coefficients, of $I(D)$, where D runs through simplices with vertices in $V(P)$. This can be viewed as a non-convex generalisation of triangulations of convex polytopes.

4.15 Optimal proving algorithms

Edward A. Hirsch (Steklov Institute – St. Petersburg, RU)

Joint work of Edward A. Hirsch, D. Itsykson, I. Monakhov, A. Smal

The existence of a (p)-optimal propositional proof system is a major open question in (proof) complexity; Krajíček and Pudlák (1989) show that this question is equivalent to the existence of an algorithm (acceptor) that is optimal on all propositional tautologies.

We show that in the presence of errors such optimal algorithms *do* exist. The concept is motivated by the notion of heuristic algorithms. Namely, we allow the algorithm to claim a small number of false "theorems" (according to any polynomial-time samplable distribution on non-tautologies) and err with bounded probability on other inputs.

This construction can be viewed as "physical" proof as opposed to "mathematical" proof: the validity of a candidate algorithm is established using an "experiment" (drawing non-theorems at random and feeding them to the algorithm).

4.16 On the intersection of a sparse curve and a low-degree curve: A polynomial version of the lost theorem

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 $d \geq 1$, $G \in \mathbb{R}[X,Y]$ and 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.

4.17 Another subtraction-free algorithm for computing Schur functions

Éric Schost (University of Western Ontario – London, CA)

In recent work, Fomin, Grigoriev and Koshevoy give subtraction-free algorithms for the computation of Schur functions (and some of their generalizations), following earlier works by Koev and Demmel. In this talk, we present another algorithm, which is hinted at as a remark in Fomin et al.'s paper.

4.18 On nearly optimal algorithms for computing roadmaps of real algebraic sets

Mohab Safey El Din (UPMC – Paris, FR)

Joint work of Mohab Safey El Din, Éric Schost

Canny introduced roadmaps of semi-algebraic sets as a key tool for reducing connectivity queries in arbitrary dimension to connectivity queries on 1-dimensional semi-algebraic sets. Indeed, roadmaps are (semi-)algebraic curves which have a connected intersection with all connected components of the semi-algebraic set under consideration (and contain the query-points).

In 2010, we introduced a new technique for computing roadmaps improving the long-standing complexity bounds derived from Canny-like procedures for computing roadmaps. This has led to several developments by Basu et al.

We obtained recently the first nearly optimal algorithm, i.e. running in time $D^{O(n \log(n))}$ when the input is an n-variate reduced regular sequence of degree $\leq D$ defining a smooth and bounded real algebraic set.

In this talk, we show how to remove the boundedness assumption and report on first practical results, showing that roadmaps can now be computed in practice for non-trivial examples.

4.19 Fast Multiplication of Polynomials over Arbitrary Rings

Erich Kaltofen (North Carolina State University – Raleigh, US)

As a nostalgic reprise of the time when Dima Grigoriev and I were young researchers, and in the memory of my co-author David G. Cantor (1935–2012), I will repeat my 1987 talk at Zürich, with overhead transparencies and such, on the algebraic complexity of polynomial multiplication.

I will also mention Mark Giesbrecht's 1997 application of one of our ideas to computing integral solutions to sparse systems of linear equations, and recent results based on Martin Führer's fast integer multiplication algorithm.

Unfortunately, unlike the matrix multiplication exponent, the

$$O(n \log(n) \log\log(n))$$

complexity still seems to remain the best after those 28 years.

4.20 Conic integral geometry and applications

Martin Lotz (Manchester University, GB)

Integral geometry and geometric probability, going back to the work of Blaschke and Santaló, deal with measures on spaces of geometric objects, and can answer questions about the

probability that random geometric objects intersect. We discuss various applications of (spherical) integral geometry: from the complexity theory of conic optimization to the analysis of convex optimization approaches to solving underdetermined systems of equations. In particular, it is shown how integral geometry naturally gives rise to a complete explanation of phase transition phenomena for the applicability of convex regularization to data recovery problems. We also introduce combinatorial methods, based on the theory of hyperplane arrangements, to compute the conic intrinsic volumes of various cones of interest.

4.21 Sum of squares certificates for containment of H-polytopes in V-polytopes

Thorsten Theobald (Goethe-Universität Frankfurt am Main, DE)

Joint work of Thorsten Theobald, Kai Kellner

Given an H-polytope P and a V-polytope Q, the decision problem whether P is contained in Q is co-NP-complete. This hardness remains if P is restricted to be a standard cube and Q is restricted to be the affine image of a cross polytope. While this hardness classification by Freund and Orlin dates back to 1985, there seems to be only limited progress on that problem so far.

Based on a formulation of the problem in terms of a bilinear feasibility problem, we study sum of squares certificates to decide the containment problem. These certificates can be computed by a semidefinite hierarchy. As a main result, we show that under mild and explicitly known preconditions the semidefinite hierarchy converges in finitely many steps. In particular, if P is contained in a large V-polytope Q (in a well-defined sense), then containment is certified by the first step of the hierarchy.

4.22 Topological lower bounds for computation trees and arithmetic networks

Nicolai Vorobjov (University of Bath, GB)

Joint work of Nicolai Vorobjov, Andrei Gabrielov

We prove that the height of any algebraic computation tree for deciding membership in a semialgebraic set $\Sigma \subset \mathbb{R}^n$ is bounded from below by

$$\frac{c_1 \log(\mathrm{b}_m(\Sigma))}{m+1} - c_2 n,$$

where $\mathrm{b}_m(\Sigma)$ is the m-th Betti number of Σ with respect to "ordinary" (singular) homology, and $c_1,\ c_2$ are some (absolute) positive constants. This result complements the well known lower bound by Yao for *locally closed* semialgebraic sets in terms of the total *Borel-Moore* Betti number.

We also prove that if $\rho : \mathbb{R}^n \to \mathbb{R}^{n-r}$ is the projection map, then the height of any tree deciding membership in Σ is bounded from below by

$$\frac{c_1 \log(\mathrm{b}_m(\rho(\Sigma)))}{(m+1)^2} - \frac{c_2 n}{m+1}$$

for some positive constants $c_1,\ c_2$.

We illustrate these general results by examples of lower complexity bounds for some specific computational problems.

An analogous theory is developed for *arithmetic networks*, a computational model aimed to capture the idea of a parallel computation in its simplest form. Here we generalize lower bounds of Montaña, Morais and Pardo (who considered locally closed semialgebraic sets relative to Borel-Moore homology) to arbitrary semialgebraic sets relative to singular homology.

5 Open Problems

The open problems session was held on Tuesday, the 9th of June.

5.1 Determinantal Witnesses and Matchings

Marek Karpinski (Universität Bonn, DE)

Given a bipartite graph $G = (V, E)$ with n vertices and the adjacency matrix $A = [a_{ij}]$. Existence of a perfect matching in G is equivalent to checking the identity to zero of a symbolic determinant $S = \mathrm{Det}([a_{ij}x_{ij}])$. Evaluate S at the points $((p_{11})^i, \ldots, (p_{nn})^i)$ for i between 1 and $n!$ and p_{jk} being "consecutive" prime numbers. Denote the values of a symbolic determinant S at those points by a_i.

It is known that existence of a matching in G is equivalent to the existence of an index $i,\ 1 \leq i \leq n!$, such that the number a_i is nonzero (Grigoriev, Karpinski 1987). Define a *determinantal witness* wt (G) of G to be a minimal index i with that property, and the n-dimensional witness wt_n to be a maximum of the determinatal witnesses of all graphs with n vertices.

Give an explicit construction of a bipartite graph such that $\mathrm{wt}(G) \geq 4$. Can the upper bound $n!$ on wt_n be reduced to a subexponential (or even polynomial) bound? Shedding some light on those issues will constitute a significant progress in the area.

5.2 Complexity of solving tropical or min-plus linear systems

Dima Grigoriev (Lille I University, FR)

A min-plus linear system has a form

$$\min_{1 \leq j \leq n} \{a_{ij} + x_j\} = \min_{1 \leq j \leq n} \{b_{ij} + x_j\},\ 1 \leq i \leq m$$

where the integer coefficients a_{ij}, b_{ij} fulfil bounds $|a_{ij}|, |b_{ij}| < M$. Solvability is asked in integers. This class of systems is polynomially equivalent to tropical linear systems and to mean pay-off games.

The long-standing question is in existence of a polynomial complexity (so, polynomial in $n, m, \log M$) algorithm for solving min-plus (or tropical) linear system. The known algorithms have complexity polynomial either in n, m, M or in $n^m, \log M$.

5.3 Construction of explicit disperser $f : \{0,1\}^n \to \{0,1\}^{o(n)}$

E. A. Hirsch (Steklov Institute – St. Petersburg, RU)

Construct an explicit disperser $f : \{0,1\}^n \to \{0,1\}^{o(n)}$ of the following kind: f should be non-constant on every possible set of solutions of size at least $2^{n/100}$ of a set of $O(n)$ quadratic equations over $\mathbb{F}_2$.

5.4 Conjecture: Log-concavity of conic intrinsic volumes

Dennis Amelunxen (City University – Hong Kong, HK)

If $C \subseteq \mathbb{R}^d$ is a (convex) polyhedral cone then its kth intrinsic volume can be defined as the probability that the projection onto the cone of a uniformly random point on the unit sphere falls into the relative interior of a k-dimensional face of C:

$$v_k(C) = \mathrm{Prob}\{\Pi_C(\mathbf{p}) \in \mathrm{relint}(F) |\ F \text{ } k\text{-dimensional face of } C\},$$

where $\Pi_C(\mathbf{z}) = \mathbf{x}$ with $\|\mathbf{z} - \mathbf{x}\| = \min\{\|\mathbf{z} - \mathbf{y}\| \mid \mathbf{y} \in C\}$ and $\mathbf{p} \sim \mathrm{Uniform}(S^{d-1})$.

(For more information about conic intrinsic volumes see `arXiv:1412.1569` and the references given therein.)

Conjecture: The intrinsic volumes of a cone form a log-concave sequence.

In technical terms, if $C \subseteq \mathbb{R}^d$ closed convex cone, then for all $1 \leq k \leq d-1$,

$$v_k(C)^2 \geq v_{k-1}(C)\, v_{k+1}(C).$$

It is known that these inequalities hold in dimension $d \leq 4$ (which in connection with the stability of log-concavity under convolution yields an infinite set of positive examples in any dimension), and recent investigations about the behavior of the intrinsic volumes in high dimensions support the plausibility of these inequalities. A proof of this conjecture could be seen as a conic analog of the famous Alexandrov-Fenchel inequalities.

5.5 Lower bounds for sums of powers of degree 1 univariate polynomials

Pascal Koiran (ENS – Lyon, FR)

We consider representations of polynomials $f \in K[X]$ under the form

$$f(X) = \sum_{i=1}^{k} \alpha_i (x + a_i)^{e_i}.$$

The problem is to find explicit polynomials f of degree d which require at least $k = \Omega(d)$ terms in any representation of this form. Such polynomials are known for the field $K = \mathbb{R}$, but the problem seems to be open for $K = \mathbb{C}$. Some background can be found in the paper "lower bounds by Birkhoff interpolation" (in preparation).

5.6 Sign-representation

Vladimir Podolskii (Steklov Institute – Moscow, RU)

Consider a sequence of Boolean functions $\{f_n\}_{n\in\mathbb{N}}$, where $f_n \colon \{1,2\}^n \to \{-1,1\}$. We say that polynomials $p_n \in \mathbb{Z}[x_1,\dots,x_n]$ sign-represent this sequence of functions if for all n and for all $\mathbf{x} \in \{1,2\}^n$ we have $f_n(\mathbf{x}) = \operatorname{sign} p_n(\mathbf{x})$.

Suppose we know that the sequence $\{f_n\}_{n\in\mathbb{N}}$ can be sign-represented by a sequence of polynomials $\{p_n\}_{n\in\mathbb{N}}$ with the number of monomials growing polynomially in n. Can we say that the same sequence of functions can be sign-represented by a sequence of polynomials with polynomial number of monomials and with any bound on the degree?

The background on the problem can be found in the paper http://eccc.hpi-web.de/report/2013/021/.

5.7 Complexity of testing membership to Kronecker polytopes

Peter Bürgisser (TU Berlin, DE)

Kronecker coefficients play a crucial role in geometric complexity theory for proving lower bounds for tensor rank and determinantal complexity.

Let λ, μ, ν be three partitions of k into at most n parts. The Kronecker coefficient $g(\lambda,\mu,\nu)$ is the multiplicity of the irreducible $\mathrm{GL}_n(\mathbb{C})^3$-representation of type (λ,μ,ν) in the the space of forms of degree k on $\mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^n$. Let $\Delta(n)$ denote the closure of the set of $\frac{1}{k}(\lambda,\mu,\nu)$ such that $g(\lambda,\mu,\nu) > 0$. It is known that $\Delta(n)$ is a convex polytope. We study the problem KRON – POLYTOPE of testing membership to $\Delta(n)$ for given partitions λ, μ, ν, each given as a list of n integers encoded in binary (n is varying and part

of the input). Recently, it was shown by Bürgisser, Christandl, Mulmuley, and Walter that $\mathrm{KRON} - \mathrm{POLYTOPE} \in \mathrm{NP} \cap \mathrm{coNP}$.

Is there a polynomial time algorithm for testing membership to Kronecker polytopes?

5.8 Cylindrical decomposition with topologically regular cells

Nicolai Vorobjov (University of Bath, GB)

Let $X \subset \mathbb{R}^n$ be a bounded set definable in an o-minimal structure over the reals, e.g., a semialgebraic or a subanalytic set. It is well known that $\mathbb{R}^n$ admits a cylindrical cell decomposition compatible with X. It is obvious from the definition that each cell of the decomposition is a *topological cell*, i.e., a homeomorphic image of a standard open ball. However, there are examples (see Section 4 in S. Basu, A. Gabrielov, and N. Vorobjov, J. European Math. Soc., 15, 2, 2013, 635-657) when a definable cylindrical cell is not *topologically regular*[1].

Conjecture: For any definable bounded $X \subset \mathbb{R}^n$ there is a cylindrical cell decomposition of $\mathbb{R}^n$, compatible with X, such that each cell, contained in X, is topologically regular.

This conjecture is proved in two cases: $\dim X \leq 2$ and $\dim X = 3,\ n = 3$ (S. Basu, A. Gabrielov, and N. Vorobjov, `arXiv:1402.0460`).

[1] A set Y is called *topologically regular cell* if the pair $(\overline{Y}, Y)$ is homeomorphic to the pair $(\overline{B}, B)$, where B is the standard open ball, and the bar denotes the closure operation.

Participants

- Dennis Amelunxen
City Univ. – Hong Kong, HK
- Saugata Basu
Purdue University – West Lafayette, US
- Peter Bürgisser
TU Berlin, DE
- Michel Coste
University of Rennes, FR
- Felipe Cucker
City Univ. – Hong Kong, HK
- James H. Davenport
University of Bath, GB
- Dima Grigoriev
Lille I University, FR
- Edward A. Hirsch
Steklov Institute – St. Petersburg, RU
- Erich Kaltofen
North Carolina State University – Raleigh, US
- Marek Karpinski
Universität Bonn, DE
- Pascal Koiran
ENS – Lyon, FR
- Martin Lotz
Manchester University, GB
- Klaus Meer
BTU Cottbus, DE
- Friedhelm Meyer auf der Heide
Universität Paderborn, DE
- Dmitrii V. Pasechnik
University of Oxford, GB
- Vladimir Podolskii
Steklov Institute – Moscow, RU
- Ilia Ponomarenko
Steklov Institute – St. Petersburg, RU
- Natacha Portier
ENS – Lyon, FR
- Marie-Françoise Roy
University of Rennes, FR
- Mohab Safey El Din
UPMC – Paris, FR
- Éric Schost
University of Western Ontario – London, CA
- Vladimir Shpilrain
City University of New York, US
- Anatol Slissenko
Université Paris-Est Créteil, FR
- Thorsten Theobald
Goethe-Universität Frankfurt am Main, DE
- Nicolai Vorobjov
University of Bath, GB
- Andreas Weber
Universität Bonn, DE