04061 Abstracts Collection
Real Computation and Complexity
— Dagstuhl Seminar —

Thomas Lickteig[1], Klaus Meer[2] and Luis Miguel Pardo[3]

[1] Univ. Limoges, FR
thomas.lickteig@unilim.fr
[2] Univ. Southern Denmark, DK
meer@imada.sdu.dk
[3] Univ. de Cantabria, ES
luis.pardo@unican.es

Abstract. From 01.02.04 to 06.02.04, the Dagstuhl Seminar 04061 "Real Computation and Complexity" was held in the International Conference and Research Center (IBFI), Schloss Dagstuhl. During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. Abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in this paper. The first section describes the seminar topics and goals in general. Links to extended abstracts or full papers are provided, if available.

Keywords. Real algebraic complexity and lower bounds, numerical methods, homotopy methods, condition as complexity ingredient, symbolic methods, bit complexity

04061 Summary – Real Computation and Complexity

The seminar "Real Computation and Complexity" was intended as a meeting place of several tendencies in the complexity analysis of algorithms in real computation.

One main idea therefore was to bring together scientists with rather different backgrounds such as numerical analysis, symbolic computing, real and complex algebraic geometry, logic, differential algebra and computational complexity.

This broadness guaranteed to get a thorough overview of current results, methods and trends in the area. It allowed as well to discuss main problems related to all aspects of real computation and complexity from different perspectives.

Joint work of: Lickteig, Thomas; Meer, Klaus; Pardo, Luis Miguel

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/499

On the average complexity of algorithms over the rationals

David Castro (Universidad de Alcalá, E)

In our talk we consider the following two questions:

1.- Is there any relationship between continuous average complexity analysis and discrete ones?

2.- Can be continuous average complexity analysis transferred to discrete ones?

We give positive answers for both of them and we state transfer principles which allow us to derive average complexity estimates in a discrete setting from similar estimates in the continuous case. Usually it is simpler to do things in a continuous setting and the moral of our talk is that, under certain assumptions, these continuous estimates reflect the practical average complexity.

We apply the transfer principles developed to the case of two different approaches to solve linear programming problems: simplex and barrier methods, obtaining that both of them are efficient for rational entries on the average. We do so, considering Brogwardt and Huhn's estimates that were done in a continuous setting.

Joint work of: Castro, David; Morais, Jose Enrique; Pardo, Luis Miguel

A Structure of Finite Signature with P=NP

Christine Gaßner (Universität Greifswald, D)

We use a uniform model of computation over structures of finite signatures. The permitted computing operations are given by the functions of the considered structure. The test conditions are defined by means of the relations of such a structure. This is a generalization of the Blum-Shub-Smale model.

The considered structure is a structure of trees which are used for structuring data for the efficient inserts and searches of data in the computer science.

The identity relation does not belong to this structure. The structure can be expanded by a relation such that P=NP is valid respecting the uniform computation model over this. The identity is decidable.

Resultant computation for polynomials in Bernstein form

Luca Gemignani (Università di Pisa, I)

We devise a fast fraction-free algorithm for the computation of the triangular factorisation of Bernstein-Bezoutian matrices with entries over an integral domain. Our approach uses the Bareiss fraction-free variant of Gaussian elimination, suitably modified to take into account the structural properties of Bernstein-Bezoutian matrices.

The algorithm can be used for solving problems in algebraic geometry that arise in computer aided geometric design and computer graphics. In particular, an example of the application to this algorithm to the numerical computation of the intersection points of two planar rational Bézier curves is presented.

Joint work of: Gemignani, Luca; Bini, D. A.; Winkler, J.

Polar Varietes, Real Elimination & Application to the Wavelet Design

Marc Giusti (Ecole Polytechnique - Palaiseau, F)

Let W be a closed algebraic subvariety of the n-dimensional projective space over the complex or real numbers and suppose that W is non-empty and equidimensional. In this talk (based on [BGHP03]) the classic notion of polar variety of W associated with a given linear subvariety of the ambient space of W is generalized. As particular instances of this new notion of generalized polar variety we reobtain the classic ones and two new types of polar varieties, called dual and (in case that W is affine) conic. In the case that the variety W is affine and smooth and has a complete intersection ideal of definition, we are able, for a generic parameter choice, to describe locally the generalized polar varieties of W by explicit equations.

We show constructively that for a generic parameter choice the generalized polar varieties of W are empty or equidimensional and smooth in any regular point of W.

Joint work of: Bank, Bernd; Giusti, Marc; Lehmann, Lutz; Heintz, Joos; Pardo, Luis Miguel

Approximate factorization of multivariate polynomials via differential equations

Erich Kaltofen (North Carolina State University, USA)

The input to our algorithm is a polynomial $f(x, y)$, whose complex rational coefficients are considered imprecise with an unknown error that causes f to be irreducible over the complex numbers CC. We seek to perturb the coefficients by a small quantitity such that the resulting polynomial factors over CC. Ideally, one would like to minimize the perturbation in some selected distance measure, but no efficient algorithm for that is known. We give a numerical multivariate greatest common divisor algorithm and use it on a numerical variant of algorithms by W. M. Ruppert and S. Gao.

Our numerical factorizer makes repeated use of singular value decompositions. We demonstrate on a significant body of experimental data that our algorithm is practical and can find factorizable polynomials within a distance that

is about the same in relative magnitude as the input error, that even when the relative error in the input is substantial (10^{-5}).

Joint work with Shuhong Gao (Clemson), John P. May (NCSU), Zhengfeng Yang and Lihong Zhi (AMSS Beijing)

Keywords: Polynomial factorization, numerical greatest common divisor, approximate coefficients, singular value decomposition, Maple software

Joint work of: Gao, Shuhong; Kaltofen, Erich; May, John P.; Yang, Zhengfeng and Zhi, Lihong

Σ-definability and Computability on Continuous Data Types

Margarita Korovina (A. P. Ershov Institute - Novosibirsk, RUS)

It is well-known that the classical theory of computation, which works with discrete structures,is not suitable for formalisation of computations that operate on real-valued data. Most computational problems in physics and engineering are of this type, e.g. problems relevant to foundation of dynamical and hybrid systems.

Since computational processes are discrete in their nature and objects we consider are continuous, formalisation of computability of such objects is already a challenging research problem.

In this talk we will report about logical approach to computability on the reals based on the notion of definability. In this approach continuous objects and computational processes involving these objects can be defined using finite formulas in a suitable structure.

We will discuss beneficial features of this approach, recent results and future work.

On Existence and Approximation of Clusters of Zeros: Case of Embedding Dimension One

Grégoire Lecerf (Université de Versailles, F)

In the beginning of the eighties, S. Smale developed a quantitative analysis of Newton's method for multivariate analytic maps. In particular, his alpha-theory gives an effective criterion that ensures safe convergence to a simple isolated zero, i.e. where the map has corank zero. This criterion requires only information concerning the map at the initial point of the iteration. Generalizing this theory to multiple zeros is still a challenging problem. In this talk we deal with situations where the analytic map has corank one at the multiple zero, which has embedding dimension one. More generally, we define clusters of embedding dimension one.

We provide a criterion for detecting such clusters of zeros and a fast algorithm for approximating them, with quadratic convergence. In the case of a cluster with positive diameter this algorithm stops at a distance of the cluster which is about its diameter.

Joint work of: Giusti, Marc; Salvy, Bruno; Yakoubsohn, Jean-Claude

Bilinear splitting formulas for graph polynomials

Johann Makowsky (Technion - Haifa, IL)

Department of Computer Science, Technion-IIT, Haifa, Israel We give an overview and unify various techniques of computing graph polynomials efficiently on input which satisfy various structural properties. The abstract, and only theoretically efficient, version of the technique is based on a generalization of the Feferman-Vaught theorem for Monadic Second Order Logic.

Practically efficient versions include the Tutte polynomial and colored Tutte polynomials, the generating function for SAT and others.

On the Curvature of the Central Path of Linear Programming Theory

Gregorio Malajovich (UFRJ - Rio de Janeiro, BR)

We prove a linear bound on the average total curvature of the central path of linear programming theory in terms on the number of independent variables of the primal problem, and independent on the number of constraints.

Joint work of: Malajovich, Gregorio; Dedieu, J-P.; Shub, M.

Numeric vs. symbolic homotopy algorithms in polynomial equation solving: a case study

Guillermo Matera (University of Buenos Aires, RA)

We consider a family of polynomial equation systems which arises in the analysis of the stationary solutions of a standard discretization of certain semilinear second order parabolic partial differential equations. We prove that this family of systems is well–conditioned from the numeric point of view, and ill–conditioned from the symbolic point of view. We exhibit a polynomial–time numeric algorithm solving any member of this family, which significantly contrasts the exponential behaviour of all known symbolic algorithms solving a generic instance of this family of systems

Joint work of: De Leo, M.; Dratman, E.

An Evolutionary Algorithm for Solving Word Equation Systems

Jose Luis Montana (University of Cantabria, E)

In 1977 Makanin stated that the solvability problem for word equation systems is decidable.

Makanin's algorithm is very complicated and the solvability problem for word equations remains NP-hard even if one looks for short solutions. We show that testing solvability of word equation systems is a NP-complete problem if we look for solutions of length bounded by some given constant greater than or equal to two over some single letter alphabet. We propose a local search genetic algorithm for this problem and give some experimental results which indicate that our approach to this problem becomes a promising strategy.

Keywords: Evolutionary computation, genetic algorithms, huristic local search

Joint work of: Montana, Jose Luis; Alonso, C; Drubi, F.

Solving Integral Equations Using Random Bits

Erich Novak (Universität Jena, D)

Integral equations with Lipschitz kernels and right-hand sides are intractable for deterministic methods, the complexity increases exponentially in the dimension d.

This is true even if we only want to compute a single function value of the solution.

For this latter problem we study coin tossing algorithms (or restricted Monte Carlo methods), where only random bits are allowed.

We construct a restricted Monte Carlo method with error ϵ that uses roughly ϵ^{-2} function values and only $d \log^2 \epsilon$ random bits. The number of arithmetic operations is of the order $\epsilon^{-2} + d \log^2 \epsilon$.

Hence, the cost of our algorithm increases only mildly with the dimension d, we obtain the upper bound $C \cdot (\epsilon^{-2} + d \log^2 \epsilon)$ for the complexity.

In particular, the problem is tractable for coin tossing algorithms.

Joint work of: Novak, Erich; Pfeiffer, Harald; Heinrich, Stefan

A new method for cell decomposition of restricted subanalytic sets

Sawas Perikleous (Université de Rennes, F)

We present a method which decomposes the closed unit cube $I^n \subset \mathbb{R}$ into a disjoint union of cylindrical cells, compatible with a given semianalytic subset $S \subset I^n$, in such a way that if S is described by members of any family of restricted analytic functions closed under addition, multiplication and taking partial derivatives, then each cell of the decomposition is a subanalytic set described by functions from the same family. In the important particular case when the analytic functions involved in the definition of S come from a certain broad finitely defined class (namely, the class of Pfaffian functions) we are able to actually construct an algorithm for producing such a cylindrical cell decomposition, provided we are given an oracle for deciding emptiness of semi-Pfaffian sets.

This implies the possibility of effective elimination of one sort of quantifiers from a first-order formula involving restricted Pfaffian functions.

The complexity of the algorithm as well as the bounds on parameters of the output are doubly exponential in $O(n^2)$ and are the best up-to-date.

Keywords: Pfaffian functions, cell decomposition, complexity

Joint work of: Perikleous, Sawas; Vorobjov, Nicolai

Two situations with unit-cost: ordered abelian semi-groups and some commutative rings

Mihai Prunescu (Universität Freiburg, D)

The talk presents two situations where unit-cost complexity results are closely related with results from the classical computability.

- In the first part we study an important theorem by Pascal Koiran and Hervé Fournier from an axiomatic point of view. It is proved that the algebraic Knapsack problem belongs to P over some ordered abelian semi-group iff $P = NP$ clasically. In this case there would exist a unit-cost machine solving the algebraic Knapsack problem over all ordered abelian semi-groups in some uniform polynomial time.
- In the second part we apply the theorem of Matiyasevich in order to construct a ring with $P \neq NBP \neq NP$ and such that its polynomial hierarchy does not collapse at any level.

Non-Universal Algorithms to Solve Sytems of Polynomial Equations

Jorge San Martin Corujo (Universidad Rey Juan Carlos - Móstoles, E)

In this talk, I introduce the notion of Non–Universal Algorithm applied to the problem of solving systems of multivariate polynomial equations. Roughly speaking, such algorithms do not compute full information on the solution variety, but only a piece of it.

I exhibit two different approaches: a symbolic procedure and a numerical one. In the first case, a symbolic algorithm is presented to solve a very general family of polynomial systems, the so called Generalised Pham Systems.

In the second case, we study the complexity of the Numerical Linear Homotopy Deformation Algorithm within the context of the Approximate Zero Theory under the classical Turing Machine Model.

Joint work of: San Martin Corujo, Jorge; Beltrán, C.; Pardo, Luis Miguel

Fast Algorithms for Computing exp, ln, sin, cos at Medium Precision

Arnold Schönhage (Universität Bonn, D)

Low precision methods for the elementary functions are well established in modern computer hardware, high precision methods are based on the AGM, see Borwein & Borwein, "Pi and the AGM".

Here we present a new idea for medium precision of 50-2500 bits, say. Standard domain reductions like $x' = x - n.ln2$ for exp, $x' = x.2^n$ in [1,2) for ln, $x' = x - n.pi/2$ for $cos + i.sin$ plus Taylor approximations are combined with further reductions by diophantine combinations of incommensurable logarithms, like $z = x' - (k.ln3 - m.ln2)$ for exp, or $z = x' - (+ - k.arctan(1/2) - m.pi/4)$ for cos, sin, with small |z| and subsequent multiplication by 3^k, or by $(2 + -i)^k.e^i z/5^(k/2)$, respectively. Variations of this idea are discussed.

Shifted number systems for safe seminumeric computation

Arne Storjohann (University of Waterloo, CDN)

Exact linear algebra computations on integer matrices, like linear system solving, can be speeded by using approximate arithmetic. For example, the leading coefficient of the p-adic expansion of the product of two integer may be recovered from the first few leading coefficients of the operands. Unfortunately, the phenomenon of integer carries may lead to errors. The shifted number system gives a method for detecting error-producing carries, together with a method, based on a single random shift choice, for bounding the probability of such egregious carries.

Numerical Decomposition of the Intersection of Algebraic Varieties

Jan Verschelde (Univ. of Illinois - Chicago, USA)

In a recent joint work with Andrew J. Sommese (University of Notre Dame) and Charles W. Wampler (General Motors Research and Development) we have developed numerical homotopy methods to decompose positive dimensional solution sets of polynomial systems into irreducible components.

The problem addressed in this talk is the intersection of two irreducible solution components of two possibly identical polynomial systems, a problem which could not be solved by any previous numerical homotopy.

To develop new homotopies to solve this problem, we generalize our algorithms for a numerical irreducible decomposition to polynomial systems restricted to an algebraic set. Considering the diagonal system of equations u - v = 0 restricted to the product of the two components we wish to intersect leads to the "diagonal homotopy", providing a numerical representation of the intersection. Computational experiments illustrate the efficiency of this new diagonal homotopy.

Joint work of: Verschelde, Jan; Sommese, Andrew J.; Wampler, Charles W.

Betti numbers of definable sets

Nicolai Vorobjov (University of Bath, GB)

The talk presents the new upper bounds on Betti numbers of definable sets, including semialgebraic and sub-Pfaffian sets, described by quantifier-free formulae and formulae with quantifiers. The main technical tool is a spectral sequence converging to the homologies of the image of a definable set.

Joint work of: Vorobjov, Nicolai; Gabrielov, A.; Zell, T.

Towards a Higher Level Programming Language for Analysis

Klaus Weihrauch (FernUniversität in Hagen, D)

This is a talk on the foundation of real number computation and complexity.

Some models for defining computability in Analysis can be refined naturally to a definition of a programming language with syntax and semantics.

Still none of these programming languages seems to be satisfactory.

Either they work only on a small subset of the real numbers, they are unrealistic or they are of very low level like Turing machines.

In the talk ingredients will be presented for a realistic higher level programming language on the real numbers and higher types, where a type is an equivalence class of multi-representations.