Mathematisches Forschungsinstitut Oberwolfach

Report No. 54/2012

DOI: 10.4171/OWR/2012/54

Complexity Theory

Organised by
Peter Bürgisser, Paderborn
Oded Goldreich, Rehovot
Madhu Sudan, Cambridge MA
Salil Vadhan, Cambridge MA

11 November – 17 November 2012

Abstract. Computational Complexity Theory is the mathematical study of the intrinsic power and limitations of computational resources like time, space, or randomness. The current workshop focused on recent developments in various sub-areas including arithmetic complexity, Boolean complexity, communication complexity, cryptography, probabilistic proof systems, and pseudorandomness. Many of the developments are related to diverse mathematical fields such as algebraic geometry, combinatorial number theory, probability theory, representation theory, and the theory of error-correcting codes.

Mathematics Subject Classification (2000): 68-06, 68Q01, 68Q10, 68Q15, 68Q17, 68Q25, 94B05, 94B35.

Introduction by the Organisers

The workshop *Complexity Theory* was organized by Peter Bürgisser (Universität Paderborn), Oded Goldreich (Weizmann Institute), Madhu Sudan (MIT and Microsoft Research), and Salil Vadhan (Harvard). The workshop was held on November 11th–17th 2012, and attended by approximately 50 participants spanning a wide range of interests within the field of Computational Complexity. The plenary program, attended by all participants, featured fifteen long lectures, an open problem session, and ten short (5-minute) reports mostly by students and postdocs. In addition, intensive interaction took place in smaller groups.

The Oberwolfach Meeting on Complexity Theory is marked by a long tradition and a continuous transformation. Originally starting with a focus on algebraic and Boolean complexity, the meeting has continuously evolved to cover a wide variety

of areas, most of which were not even in existence at the time of the first meeting (in 1972). While inviting many of the most prominent researchers in the field, the organizers try to identify and invite a fair number of promising young researchers.

Computational complexity (a.k.a. complexity theory) is a central field of computer science with a remarkable list of celebrated achievements as well as a vibrant research activity. The field is concerned with the study of the *intrinsic complexity* of computational tasks, and this study tends to *aim at generality*: it focuses on natural computational resources, and considers the effect of limiting these resources on the class of problems that can be solved. Computational complexity is related to and has substantial interaction with other areas of mathematics such as algebra, analysis, combinatorics, geometry, number theory, optimization, probability theory, and quantum computation.

The workshop focused on several sub-areas of complexity theory and its nature may be best illustrated by a brief survey of some of the meeting's highlights.

Matrix Multiplication. The Oberwolfach meeting on complexity theory that took place in 1979 is famous for Strassen's presentation of his landmark subcubic time algorithm for matrix multiplication and a sequence of improvements that followed via interaction of several participants in that meeting. In connection with that tradition, Virginia Vassilevska Williams presented her recent algorithmic improvement that breaks the record set in 1987 by Coppersmith and Winograd. Her improvement is based on structural results regarding the mathematical objects that arise in the Coppersmith and Winograd algorithm, which lend themselves to an automatic search for better objects (using convex and nonconvex optimization).

Chris Umans reported on the state of his on-going project for designing better matrix multiplication algorithms. In particular, a generalization of the group-theoretic approach to using "coherent configurations" seems to facilitate further progress in this project, which has a potential of obtaining almost-optimal (i.e., quadratic-time) algorithms. So far, however, the group-theoretic approach was only able to get close to the best upper bounds known (but did not quite meet them, let alone supersede them).

Boolean Circuit Lower Bounds. The project of establishing circuit lower bounds calls for presenting (relatively) explicit functions that cannot be computed within limited computational resources. Ryan Williams presented the most significant progress in circuit lower bounds since the 1980s, proving that there exists a function in non-deterministic exponential-time (i.e., in the complexity class NE) that cannot be computed by polynomial-size Boolean circuits of constant depth with modular gates (i.e., the class ACC). The breakthrough is in proving a lower bound for less limited circuits than those considered in the past, although the level of explicitness (i.e., being in NE) is relatively weaker than in previous results.

Interestingly, his lower bound is obtained by designing an algorithm, one that slightly improves over the obvious algorithm for testing satisfiability of ACC circuits. Combined with the contradiction hypothesis (by which NE is in ACC), this algorithm yields an impossible speed-up for the class NE (i.e., one that contradicts

a known hierarchy theorem). This suggests that the fact that certain pseudorandom generators (PRGs) imply circuit lower bounds that are better than currently known does not necessarily mean that obtaining such PRGs is hopeless; it may just be a way to establishing new lower bounds.

Pseudorandom Generators. Pseudorandom generators (PRGs) are deterministic algorithms that stretch short random seeds into longer (pseudorandom) sequences that look random to distinguishers that are confined to certain complexity classes. Various notions of PRGs differ by the class of distinguishers that they fool as well as the efficiency of the PRG itself and the amount of stretch, and in some cases the construction of PRGs is related to the existence of related lower bounds (or to the assumption that such lower bounds hold).

Raghu Meka surveyed recent progress made in the study of unconditional pseudorandom generators; that is, PRGs that can be constructed without relying on any unproved computational hardness conjectures. One research direction led to optimal conversion of known results regarding computational hardness into pseudorandomness with respect to the corresponding classes (i.e., the classes capturing corresponding computational resources). The results obtained in this direction are based on a novel integration of a lower bound technique (i.e., the technique of random restrictions) in the context of PRGs. A second direction led to an almost polynomial-time deterministic algorithm for approximating the number of solutions to a given DNF formula.

Turning to hardness and pseudorandomness with respect to any efficient (i.e., probabilistic polynomial-time) computation, Benny Applebaum surveyed the construction of PRGs that are extremely easy to compute in the sense that each output bit depends on a constant number of input bits (i.e., the class NC0). One recent work, which he mentioned, shows that the assumption that certain NC0 functions are easy to compute but hard to invert (i.e., that these functions are one-way functions) implies that related functions are PRGs.

Homomorphic Encryption. A fully homomorphic encryption scheme is one that allows for arbitrary manipulation of ciphertexts without decrypting them; that is, for any polynomial-time computable function f, one can efficiently obtain an encryption of $f(x)$ when given an encryption of x (without being able to decrypt). The notion, suggested in the 1980s, was considered unimplementable till a few years ago, when first evidence to its feasibility was given. Zvika Brakerski presented the most up-to-date evidence for this feasibility, relying on the conjectured hardness of learning with errors.

Delegating Computation and Complexity theory. The possibility of delegating computation to untrusted parties relies on the possibility of verifying the correctness of such computation. For this to make sense, verification ought to be significantly faster than the original computation, whereas convincing the verifier (i.e., the proving task) should remain feasible (or relatively feasible in comparison to the original computation). Guy Rothblum presented recent progress in this direction, presenting both an interactive proof system and an interactive proof

of proximity (in the spirit of property testing) for problems in the complexity class NC.

Differential Privacy and Complexity theory. This area is concerned with the study of trade-offs between the utility available from a "sanitized" data base and the level of privacy (of individual records) preserved by such a mechanism. In principle, one should be able to extract global statistics while violating privacy to a very small extent. Results of this type started to appear less than a decade ago and a more systematic study arose in the last few years.

Moritz Hardt provided a survey of recent progress in this area, emphasizing complexity-theoretic aspects such as highly non-trivial composition theorems, connections to computational learning theory, and open questions regarding the computational complexity of some problems in differential privacy.

Machine learning (albeit in the unsupervised rather than supervised learning context) was the focus of Sanjeev Arora's presentation, which highlighted algorithmic progress and challenges in this area.

The Unique Games Conjecture. Introduced a decade ago, the unique games conjecture (UGC) states that constraint satisfaction problems involving two variables and constraints that correspond to a matching between values are hard to approximate in an extreme sense (i.e., it is infeasible to distinguish instances in which almost all constraints can be simultaneously satisfied from instances in which only few constraints can be simultaneously satisfied). Boaz Barak presented a survey of recent research on the UGC, presenting both positive and negative circumstantial evidence for the validity of UGC.

Communication Complexity. Anup Rao surveyed recent progress in communication complexity that is based on the notion of Interactive Information Complexity (IIC). The key point is that IIC allows to prove that resources must be increased when trying to solve several independent instances. This is done by showing that a protocol that solves the multi-instance problem can be transformed into a much more efficient protocol that solves a single instance, where the "complexity shrinkage" is obtained by noting that the communication in the multi-instance protocol carries relatively little information on a typical instance.

Communication complexity was also pivotal in David Steurer's presentation, where it was used to prove exponential lower bounds on the size of linear programs that solve certain natural optimization problems.

Additive Combinatorics and its Applications to Complexity. Noga Ron-Zewi's presentation focused on the Polynomial Freiman-Ruzsa conjecture and its applications to complexity theory, which are derived via the notion of approximate duality. The applications she highlighted are to the construction of two-source randomness extractors and towards proving the Log-Rank Conjecture in communication complexity.

Computational Aspects of Coding Theory. The method of multiplicities is based on the observation that the number of roots of multivariate polynomial, counted with multiplicities, does not exceed the bound commonly used for counting

roots without multiplicities. This bound is meaningful even when the total degree exceeds the size of the base field. This observation can be used in the analysis of various constructs that are based on multivariate polynomials as well as in the actual construction of locally decodable codes. Shubhangi Saraf's presentation focused on the latter case, aka Multiplicity Codes, where a multivariate polynomial (over a finite field) is encoded by its evaluation as well as by it derivatives at all points of the domain. It is remarkable that multiplicity codes, while easy to construct, can be efficiently be decoded up to the list decoding capacity.

Lower Bounds for Arithmetic Circuits Valiant conjectured in 1979 that the permanent per_n of an n by n matrix cannot be computed by arithmetic circuits of size polynomial in n. This fundamental problem of algebraic complexity is often considered the arithmetic version of P versus NP. In his talk, Pascal Koiran explained the recent progress around this question. A relatively new insight is that attention may be restricted to circuits of depth four, which means considering sums of products of sparse polynomials: more specifically, Valiant's Conjecture would follow from a lower bound $2^{\omega(\sqrt{n}\log^2 n)}$ for the size of arithmetic circuits of depth four that compute per_n. Very recently, the lower bound $2^{\Omega(\sqrt{n})}$ was obtained, which seems close to the objective. The proof of this exciting result was presented in detail in a special session by Neeraj Kayal. It relies on considering the growth of the Hilbert function of permanental ideals. There seems potential for further improvements.

Another remarkable recent result is a connection of Valiant's Conjecture to a question concerning the number of real zeros of polynomials. More specifically, the *Real Tau Conjecture* claims that the number of real zeros of a polynomial given by a depth four circuit is bounded by a polynomial in the size of the circuit. Koiran proved that this conjecture implies Valiant's Conjecture. The Real Tau Conjecture is currently wide open: There is evidence that it holds for random polynomials. Unlike its cousin, Shub and Smale's Tau Conjecture, it is not of a number-theoretic nature and so there is hope that it can be successfully attacked using tools from analysis. Some progress has been made in this direction using Wronskian determinants.

An open problem session. As part of the plenary session, Boaz Barak has organized an open problem session, which included the following presentations:

- Results and conjectures which explain why different optimization and constraint-satisfaction problems (such as 2SAT vs. 3SAT) have different complexities (Prasad Raghavendra).
- Frontiers in the construction of expander graphs (Omer Reingold).
- A conjecture regarding the inapproximability of constraint satisfaction problems where the constraints are weighted majority functions with very unbalanced weights (Johan Hastad).
- The next step in the construction of pseudorandom generators that fool depth-two circuits, or the seemingly last step that yields no new lower bound (Luca Trevisan).

In all cases, the problem was presented in its wider context, while stressing the conceptual importance of the question to this wider context.

Informal specialized sessions. Besides the formal plenary program, intense interaction between the participants took place in smaller groups. Part of these took place in the form of specialized sessions, featuring the following presentations.

- Hardness results in differential privacy (by Salil Vadhan, in continuation of Moritz Hardt's plenary presentation).
- Direct products in communication complexity (by Anup Rao, in continuation of his plenary presentation).
- Open discussion on PCPs.
- A session on Extractors, Expanders and PRGs, with talks on
  - algebraic expanders (survey by Amir Yehudayoff),
  - algebraic SL vs L (by Michael Forbes),
  - characterizing pseudoentropy (by Salil Vadhan),
  - new extractors using multiplicities (by Chris Umans, in continuation of Shubhangi Saraf's plenary presentation).
- A session on Cryptography, featuring talks on
  - functional encryption and reusable garbled circuits (by Shafi Goldwasser),
  - modulus-dimension trade-offs in the Learning with Errors problem (by Zvika Brakerski)
- Parallel Repetition Theorem for projection games (by Irit Dinur).
- Population Recovery (by Avi Wigderson).
- Explicit lower bounds via geometric complexity theory (by Christian Ikenmeyer).
- Lower bounds for depth four arithmetic circuits (by Neeraj Kayal, see our discussion of lower bounds for arithmetic circuits (above)).
- List decoding Reed–Solomon subcodes up to the singleton bound (by Venkat Guruswami).
- Locally correctable and locally decodable codes over $\mathbb{R}$ with connections to matrix rigidity (by Zeev Dvir).
- List-decoding multivariate multiplicity codes (by Swastik Kopparty, also related to Shubhangi Saraf's plenary presentation).
- The Bourgain–Gamburd–Helfgott approach to analyzing expander graphs (by Amir Yehudayoff, continuing his survey from earlier).
- The De–Mossell–Neeman proof of Borell's Theorem on noise stability in Gaussian space (by Ryan O'Donnell)
- Block-symmetric polynomials correlate with parity better than symmetric (by Emanuele Viola)
- PRGs from shrinkage (by Raghu Meka, in continuation of his plenary presentation).

Workshop: Complexity Theory

Table of Contents