Executive Summary of Dagstuhl Seminar 09421 on

Algebraic Methods in Computational Complexity

October 11 to 16, 2009

organized by

Manindra Agrawal
Lance Fortnow
Thomas Thierauf
Chris Umans

The seminar brought together more than 50 researchers covering a wide spectrum of complexity theory. The focus on algebraic methods showed once again the great importance of algebraic techniques for theoretical computer science. We had almost 30 talks, most of them about 40 minutes leaving ample room for discussions. We also had a much appreciated open problem session. In the following we describe the major topics in more detail.

Scott Aaronson gave the opening talk on the relationship between problems that are efficiently solvable by quantum algorithms, captured by the class BQP, and the classical polynomial time hierarchy, PH. This addresses a problem which is open since the earliest days of quantum computing. Scott presented new evidence that quantum computers can solve problems outside PH, and related the question to frontier topics in Fourier analysis, pseudorandomness, and circuit complexity.

Valentine Kabanets talked on *algebrization*, a notion introduced by Scott Aaronson and Avi Wigderson which extends the old notion of *relativization* considerably. Since the 1970s we know that we need non-relativizing techniques to separate complexity classes like P and NP. Since then, a few techniques have been developed that indeed don't relativize. However, Scott and Avi showed that all these techniques *algebrize*, but that we need non-algebrizing techniques to separate P from NP. Hence they have established a new barrier. Valentine proposed an axiomatic approach to algebrization, which complements and clarifies the approach of Scott and Avi. He presented logical theories formalizing the notion of algebrizing techniques so that most algebrizing results are provable within these theories and separations requiring non-algebrizing techniques are independent of them.

Algorithms that use only small amount of space draw much attention these days. Meena Mahajan proposed an algebraic variant of deterministic log-space which is motivated by Valiant's algebraic model of computation.

Dagstuhl Seminar Proceedings 09421
Algebraic Methods in Computational Complexity
http://drops.dagstuhl.de/opus/volltexte/2010/2410

A great result was presented by Fabian Wagner: the graph isomorphism problem (GI) for planar graphs can be solved in logspace. This has to be contrasted with the fact that for general GI, we don't even have a polynomial time algorithm. He also showed that the result can be extended to K_5-free and $K_{3,3}$-free graphs.

We had a number of talks on coding theory and PCPs. Eli Ben-Sasson talked on linear codes that are affine-invariant and locally testable. Eli argued that such codes must have a low rate. Sergey Yekhanin considered the Nearest Codeword Problem (NCP) which is known to be NP-complete. Sergey considerably improved the deterministic approximation algorithms known for NCP. Atri Rudra talked on the error detection problem for codes in the streaming model. Many participants were excited to hear a brand-new result of Anna Gal giving lower bounds on the rate of certain locally decodable codes, a class of codes introduced by Katz and Trevisan in 2000. For these codes it suffices to read a constant number of bits of the word received to retrieve one bit of the original input with high probability.

In an impressive talk, Dana Moshkovitz gave a very elegant algebraic proof for the low error PCP Theorem. Since she had to skip many details in the morning talk, she presented a full proof in a special evening session.

Ilan Newman talked on geometric embeddings of finite metric spaces into spaces of small dimension. The celebrated Johnson-Lindenstrauss Theorem states such an embedding for the Euclidian metric. Ilan pointed out that the situation for the ℓ_1-metric is far less understood. He defined a notion related to the dimension, the *cut-dimension*, and showed an embedding for ℓ_1 into a space of small cut-dimension.

In a one hour lecture, Nitin Saxena gave a very interesting survey-type talk on polynomial identity testing (PIT), with a focus on his own exciting results. Nitin considers polynomials described by depth-3 circuit of the form $\Sigma\Pi\Sigma$, where the top addition gate has fan-in k and the second level multiplication gates have fan-in d. Hence d is the degree of the polynomial. The circuit is associated with a matrix defined from the coefficients of the polynomial defined by the circuit. The *rank of the circuit* is defined as the rank of this matrix. If the circuit computes the zero-polynomial, the its rank is bounded. Previously, the best rank bound known was $2^{O(k^2)}(\log d)^{k-2}$ by Dvir and Shpilka (STOC 2005). This bound is exponential in k. Nitin improved this bound dramatically to $O(k^3 \log d)$. This is no longer exponential in k and is close to the optimal bound because there is a $\Omega(k \log d)$ lower bound.

Ronen Shaltiel introduced the notion of *typically-correct derandomization* of a randomized algorithm A, which is a deterministic algorithm B

(preferably of the same complexity as A) that agrees with A on *most inputs*. The standard notion of derandomization requires B to agree with A on *all* inputs. Ronen demonstrated that the relaxed goal sometimes allows better derandomization than is known for the standard notion. For example, it is possible to unconditionally simulate a randomized AC^0-algorithm by a deterministic AC^0-algorithm that succeeds on most inputs. It also allows polynomial time deterministic simulation of BPP under assumptions that are incomparable to those used in the hardness-versus-randomness tradeoffs as for example by Impagliazzo and Wigderson.

We had a series of talks on circuit complexity. Arkadev Chattopadhyay considered solution sets of systems of generalized linear equations modulo a composite integer m that is a product of two distinct primes. The main result is that such solution sets have exponentially small correlation with the boolean function MOD_q, when m and q are relatively prime. This bound is independent of the number of linear equations. As a consequence, Arkadev derives the first exponential lower bound on the size of depth-3 circuits of type MAJ of AND of MOD_m computing the function MOD_q. This solves a long standing open problem.

V. Arvind defined the *Hadamard product of multivariate polynomials* which is motivated by the Hadamard product of matrices. He studied the arithmetic circuit and branching program complexity of the product, showed several applications, and established connections to polynomial identity testing.

Michal Koucký presented a surprising upper bound for polynomial size constant depth circuits built from modular counting gates, CC^0-circuits: the AND function can be computed by uniform probabilistic CC^0-circuits that use only $O(\log n)$ random bits. This has to be contrasted with a conjecture by Barrington, Straubing and Thrien (1990) that the Boolean AND function can not be computed (deterministic) CC^0-circuits.

Ryan Williams presented a new method for exactly solving certain NP-hard search problems. The high-level idea is to encode a subset of potential solutions of a search problem with a multivariate polynomial that can be efficiently evaluated. This polynomial is then evaluated on carefully chosen points over a group algebra that will "cancel out" all non-solutions and preserve some solutions with decent probability. This basic method has led to new randomized algorithms for several fundamental problems, most notably the longest path problem.

In cryptography, *steganography* is the art of encoding secret messages into unsuspicious covertexts such that an adversary cannot distinguish the resulting stegotexts from original covertexts. Rüdiger Reischuk pointed out

that the commonly used definition of security of a stegosystem has certain pitfalls. Therefore he proposed a different notion of security which is called *undetectability*.

As is evident from the list above, the talks ranged over a broad assortment of subjects with the underlying theme of using algebraic techniques. It was very fruitful and has hopefully initiated new directions in research. Several participants specifically mentioned that they appreciated the particular focus on a common class of *techniques* (rather than end results) as a unifying theme of the workshop. We look forward to our next meeting!