Executive Summary of Dagstuhl Seminar 07411 on

Algebraic Methods in Computational Complexity

October 7 to 12, 2007

organized by

Manindra Agrawal
Harry Buhrman
Lance Fortnow
Thomas Thierauf

The seminar brought together almost 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 of length between 15 and 45 minutes. This left enough room for discussions. We had an open problem session that was very much appreciated. In the following we describe the talks in more detail.

The construction of good extractors and expanders plays a crucial role in derandomization. Chris Umans explained how to construct highly unbalanced bipartite expander graphs with expansion arbitrarily close to the degree, essentially optimal. The construction is based on the ideas underlying the recent list-decodable error-correcting codes of Parvaresh and Vardy (FOCS '05). Anup Rao considered the model that the source, a family of distributions, gives a random point from some unknown low dimensional affine subspace with a low-weight basis. This model generalizes the well studied model of bit-fixing sources. He showed how to construct new extractors for this model that have exponentially small error, a parameter that is important for applications in cryptography.

Derandomization is strongly related to proving lower bounds. In 1998, Impagliazzo and Wigderson proved a hardness vs. randomness tradeoff for BPP: if one cannot derandomize BPP, then E needs exponential size circuits. Ronen Shaltiel considered the Artur-Merlin class AM instead of BPP. He showed uniform hardness vs. randomness tradeoffs for AM that are near-optimal for the full range of possible hardness assumptions.

From another point of view Eric Allender considered the question of how close we are to proving circuit lower bounds. For example any proof that NP is not equal to TC^0 will have to overcome the obstacles identified by Razborov and Rudich in their paper on "Natural Proofs." In his talk, he pointed to some plausible way to prove that TC^0 is properly contained in

Dagstuhl Seminar Proceedings 07411
Algebraic Methods in Computational Complexity
http://drops.dagstuhl.de/opus/volltexte/2008/1306

NC^1. Another obstacle in separating complexity classes like P and NP is *relativization*. Baker, Gill, and Solovay showed that no relativizable proof can separate P from NP. Since then we have seen some non-relativizing proofs like IP = PSPACE. Scott Aaronson, together with Avi Wigderson, extended the notion of relativization to *algebraization* and showed several results including that

1. All known relevant examples of non-relativizing proofs algebrize, and
2. Any proof that separates P from NP would require non-algebrizing techniques.

We had a series of talks on circuit complexity. Fred Green gave a complete characterization of the smallest circuits that compute parity that have a majority gate as output, a middle layer of MOD_3 gates and a bottom layer of AND gates of fan-in 2. Nitin Saxena presented a deterministic polynomial time algorithm for testing whether a *diagonal* depth-3 circuit C (i.e. C is a sum of powers of linear functions) is zero. Motivated by the problem of factoring integers, Pierre Mckenzie exhibited "gems", that is, arithmetic $\{+, -, x\}$-circuits that use only n multiplication gates to compute univariate integer polynomials having 2^n distinct integer zeros, for $n = 1, 2, 3, 4$. Rüdiger Reischuk talked on bit comparator sorting circuits that have a minimal average time complexity. Ingo Wegener talked about lower bounds for the multiplication function that can be obtained by the technique of Nechiporuk. Falk Unger considered circuits with noisy gates. He showed a negative result, that formulas built from gates with two inputs, in which each gate fails with probability at least epsilon, cannot compute any function with bounded error. Wim van Dam introduced a model of algebraic quantum circuit, for all finite fields GF(q). Farid Ablayev showed how bounded error syntactic quantum branching programs can be simulated by classical deterministic branching programs

We had a wide-range of talks on classical complexity. Rahul Santhanam showed that SAT is not instance compressible unless NP is contained in coNP/poly. A language L in NP is instance compressible if there is a polynomial-time computable function f and a set A such that f reduces L to A and for each $x \in L$, $f(x)$ is of size polynomial in the witness size of x. Harry Buhrman applied this result to show that there are no sub-exponential size complete sets for NP or coNP unless NP is contained in coNP/poly. John Hitchcock presented a connection between mistake-bound learning and polynomial-time dimension. As a consequence he showed that the class E does not reduce to sparse sets under certain reductions. N. Variyam Vinodchandran presented his new result that the directed planar reachability problem is in unambiguous logarithmic space (UL). Christian Glasser talked on the relation of autoreducibility and mitoticity for polylog-space many-one reductions and log-space many-one reductions. Rocco Servedio described recent results on approximating, testing, and learning halfspaces (also known as linear threshold functions, weighted majority functions, or threshold gates). Marius Zimand showed how to reduce the length of the advice given to heuristic algorithms to approximate problems in BPTIME[sublinear].

Troy Lee gave a talk on communication complexity. He presented a direct product theorem for discrepancy, one of the most general techniques in communication complexity. Nikolai Vereshchagin studied the two party problem of randomly selecting a string among all the strings of length n. He presented protocols that have the property that the output distribution has high entropy, even when one of the two parties is dishonest and deviates from the protocol. Ben Toner considered the scenario that Alice and Bob share some bipartite d-dimensional quantum state. It is known that by performing two-outcome measurements, Alice and Bob can produce correlations that cannot be obtained classically. He showed that there is a classical protocol that can classically simulate any such correlation by using only two bits of communication. Julia Kempe considered multi-prover games where the provers share entanglement. She showed that it is NP-hard to determine, or even to approximate the entangled value of the game. In the same setting Oded Regev showed that when the constraints enforced by the verifier are 'unique' constraints (i.e., permutations), the value of the game can be well approximated by a semidefinite program for one-round games between a classical verifier and two provers who share entanglement.

Property testing deals with the question of distinguishing inputs that satisfy a given property from inputs that are far from satisfying it, using a number of queries that is as small as possible. Eldar Fischer suggested that seeking out properties that are by their nature "massively parameterized" is a worthy direction for property testing research. As an example, he considered the testability of the property of having a directed path from s to t in a graph.

Jack Lutz used connections between the theory of computing and the fine-scale geometry of Euclidean space to give a complete analysis of the dimensions of individual points in fractals that are computably self-similar.

As is evident from the list above, the talks ranged a wide area of subjects with the underlying of using algebraic techniques. It was very fruitful and has hopefully initiated new directions in research. We look forward to our next meeting!