07411 Abstracts Collection
Algebraic Methods in Computational Complexity
— Dagstuhl Seminar —

Manindra Agrawal[1], Harry Buhrman[2], Lance Fortnow[3] and Thomas Thierauf[4]

[1] Indian Inst. of Technology - Kanpur, IN
manindra@iitk.ac.in
[2] CWI - Amsterdam, NL
harry.buhrman@cwi.nl
[3] Univ. of Chicago, US
lance@fortnow.com
[4] HTW Aalen, DE
Thomas.thierauf@HTW-Aalen.de

Abstract. From 07.10. to 12.10., the Dagstuhl Seminar 07411 "Algebraic Methods in Computational 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. Computational complexity, algebra, quantum computing, (de-) randomization

07411 Executive Summary – Algebraic Methods in Computational Complexity

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.

Keywords: Computational complexity, algebra, quantum computing, (de-) randomization

Joint work of: Agrawal, Manindra; Buhrmann, Harry; Frotnow, Lance; Thierauf, Thomas

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2008/1306

Dagstuhl Seminar Proceedings 07411
Algebraic Methods in Computational Complexity
http://drops.dagstuhl.de/opus/volltexte/2008/1307

Algebrization: A New Barrier in Complexity Theory

Scott Aaronson (MIT - Cambridge, USA)

Any proof of P!=NP will have to overcome two barriers: relativization and natural proofs. Yet over the last decade, we have seen circuit lower bounds (for example, that PP does not have linear-size circuits) that overcome both barriers simultaneously. So the question arises of whether there is a third barrier to progress on the central questions in complexity theory.

In this talk we present such a barrier, which we call "algebraic relativization" or "algebrization." The idea is that, when we relativize some complexity class inclusion, we should give the simulating machine access not only to an oracle A, but also to the low-degree extension of A over a finite field or ring. We show that, while the results IP=PSPACE and MIP=NEXP fail to relativize, they nevertheless algebrize. On the other hand, we also show that any proof of P!=NP (or even P=BPP, or NEXP not in P/poly) would require non-algebrizing techniques, of which we currently have not a single example.

We also exhibit a surprising connection between algebrization and communication complexity. Using this connection, we give an MA-protocol for the Inner Product function with O(sqrt(n) log(n)) communication, and a communication complexity conjecture whose truth would imply P!=NP.

Keywords: Oracles, relativization, query complexity, communication complexity, low-degree extensions

Joint work of: Aaronson, Scott; Wigderson, Avi

Classical Simulation Complexity of Quantum Branching Programs

Farid Ablayev (Kazan State University, RUS)

We present classical simulation techniques for measure once quantum branching programs.

For bounded error syntactic quantum branching program of width w that computes a function with error δ we present a classical deterministic branching program of the same length and width at most $(1+2/(1-2\delta))^{2w}$ that computes the same function.

Second technique is a classical stochastic simulation technique for bounded error and unbounded error quantum branching programs. Our result is that it is possible stochastically-classically simulate quantum branching programs with the same length and almost the same width, but we lost bounded error acceptance property.

Keywords: Quantum algorithms, Branching Programs, Complexity

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1310

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2008/1310

How Far Are We from Proving Circuit Size Lower Bounds?

Eric Allender (Rutgers Univ. - Piscataway, USA)

Many people are pessimistic about seeing a resolution to the P vs NP question any time soon. This pessimism extends also to questions about other important complexity classes, including two classes that will be the focus of this talk: TC^0 and NC^1.

TC^0 captures the complexity of several important computational problems, such as multiplication, division, and sorting; it consists of all problems computable by constant-depth, polynomial-size families of circuits of MAJORITY gates. TC^0_d is the subclass of TC^0 solvable with circuits of depth d. Although TC^0 seems to be a small subclass of P, it is still open if $\mathrm{NP} = \mathrm{TC}^0_3$.

NC^1 is the class of problems expressible by Boolean formulae of polynomial size. NC^1 contains TC^0, and captures the complexity of evaluating a Boolean formula.

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". That is, a "natural" proof that NP is not equal to TC^0 yields a proof that no pseudorandom function generator is computable in TC^0. This is problematical, since some popular cryptographic conjectures imply that such generators do exist. This leads to pessimism about the even more difficult task of separating NC^1 from TC^0.

Some limited lower bounds are within the grasp of current techniques, however. For example, several problems in P are known to require formulae of quadratic size – but this seems to be of little use in trying to prove superpolynomial formula size. Along similar lines, it is known that, for every d, there is a constant $c > 1$ such that the formula evaluation problem (one of the standard complete problems for NC^1) requires TC^0_d circuits of size at least n^c.

It might not seem too outrageous to hope to obtain a slightly stronger lower bound, showing that there is a $c > 1$ such that this same set requires uniform TC^0 circuits of size n^c (regardless of the depth d). We show that this would be sufficient to prove that TC^0 is properly contained in NC^1. This is joint work with Michal Koucký.

NP-hard sets are exponentially dense unless co-NP in NP/poly

Harry Buhrman (CWI - Amsterdam, NL)

We show that NP-hard sets are exponentially dense unless co-NP = NP nonuniformly. This improves classic results by Mahaney and Karp-Lipton and several other results that gave evidence that NP hard sets are not polynomially sparse. Showed that for n^{1-e} Turing reduction the result is also true for NP-complete sets.

Testing massively parameterized properties

Eldar Fischer (Technion - Haifa, IL)

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.

Usually, the considered properties had a "closed" definition, such as the property of a graph being perfect, or a definition that has a parameter with a small "footprint", such as a graph being k-colorable (where k is the parameter). However, some properties were different, such as Ilan Newman's result about testing of properties recognizable by read-once branching programs - here the "parameter" is the whole branching program!

In this talk I will suggest that seeking out properties that are by their nature "massively parameterized" is a worthy direction for property testing research. I will mainly concentrate on a model introduced by Dekel, Halevy, Lachish and Newman that by its nature provides for massively parameterized properties, the graph orientation model. In it I will present a joint work with Chakraborty, Lachish, Matsliah and Newman about the testability of the property of having a directed path from s to t.

Keywords: Property testing, st-connectivity, massive parameterization

Space-Efficient Informational Redundancy

Christian Glasser (Universität Würzburg, D)

We study the relation of autoreducibility and mitoticity for polylog-space many-one reductions and log-space many-one reductions. For polylog-space these notions coincide, while proving the same for log-space is out of reach. More precisely, we show the following results with respect to nontrivial sets and many-one reductions.

- polylog-space autoreducible <=> polylog-space mitotic

- polylog-space mitotic => log-space autoreducible => $(\log n * \log\log n)$-space mitotic

- relative to an oracle, log-space autoreducible does not imply log-space mitotic

The oracle is an infinite family of graphs whose construction combines arguments from Ramsey theory and Kolmogorov complexity.

Uniqueness of Optimal Mod 3 Circuits for Parity

Frederic Green (Clark University - Worcester, USA)

We prove that the quadratic polynomials modulo 3 with the largest correlation with parity are unique up to permutation of variables and constant factors.

As a consequence of our result, we completely characterize the smallest MAJ $\circ \mathrm{MOD}_3 \circ \mathrm{AND}_2$ circuits that compute parity, where a MAJ $\circ \mathrm{MOD}_3 \circ \mathrm{AND}_2$ circuit is one that has a majority gate as output, a middle layer of MOD_3 gates and a bottom layer of AND gates of fan-in 2. We also prove that the sub-optimal circuits exhibit a stepped behavior: any sub-optimal circuits of this class that compute parity must have size at least a factor of $\frac{2}{\sqrt{3}}$ times the optimal size. This verifies, for the special case of $m = 3$, two conjectures made by Dueñez, Miller, Roy and Straubing (Journal of Number Theory, 2006) for general MAJ $\circ \mathrm{MOD}_m \circ \mathrm{AND}_2$ circuits for any odd m. The correlation and circuit bounds are obtained by studying the associated exponential sums, based on some of the techniques developed by Green (JCSS, 2004). We regard this as a step towards obtaining tighter bounds both for the $m \neq 3$ quadratic case as well as for higher degrees.

Keywords: Circuit complexity, correlations, exponential sums

Joint work of: Green, Frederic; Roy, Amitabha

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1305

Learning, Dimension, and Reducibility to Sparse Sets

John Hitchcock (University of Wyoming, USA)

A connection between mistake-bound learning and polynomial-time dimension is developed. The Winnow algorithm is applied to show that the class E does not reduce to sparse sets under certain reductions.

Joint work of: Harkins, Ryan C.; Hitchcock, John M.

On the value of entangled games

Julia Kempe (Tel Aviv University, IL)

Multi-prover games play a central role in complexity theory. One of the key questions is to understand their power when the provers share entanglement. We show for the first time a lower bound: It is NP-hard to decide if the entangled value of the game is 1. We then proceed to show that approximating the value of such games to within a small epsilon is NP hard. On the way we present the "almost commuting" versus "nearly commuting" conjecture which captures the bottleneck to improving epsilon.

Based on joint work with Hirotada Kobayashi, Keiji Matsumoto, Ben Toner and Thomas Vidick

Direct product theorem for discrepancy

Troy Lee (Rutgers Univ. - Piscataway, USA)

We show a direct product theorem for discrepancy, one of the most general techniques in communication complexity. Namely, we show that disc(f+g) <= 8 disc(f) disc(g), for any functions f,g. This answers an open problem of Shaltiel.

Keywords: Communication complexity

Joint work of: Lee, Troy; Spalek, Robert

Dimensions of Points in Self-Similar Fractals

Jack H. Lutz (Iowa State University, USA)

We use nontrivial 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.

Joint work of: Lutz, Jack H.; Mayordomo, Elvira

Few gate but many zeros

Pierre McKenzie (Université de Montréal, CA)

Motivated by the problem of factoring integers, for $n = 1, 2, 3, 4$we exhibit "gems", that is, arithmetic $+, -, x$-circuits that use only n multiplication gates to compute univariate integer polynomials having 2^n distinct integer zeros. Our gems use n addition gates, and we show they are optimal as skew gems, where skewness imposes that each + gate has at most one non-constant input. We leave open the question whether gems exists for n greater than 4, but we show that optimal skew gems for n=5 would provide new solutions to the old number-theoretic Prouhet-Tarry-Escott problem.

Keywords: Integer factoring, algebraic circuits, univariate integer polynomials

Joint work of: Borchert, Bernd; McKenzie, Pierre; Reinhardt, Klaus

Extractors for Low-Weight Affine Sources.

Anup Rao (Univ. of Texas at Austin, USA)

Given a family of distributions (aka sources) an extractor E for the family is a function for which E(X) is close to uniform for every X in the family.

In this talk, we assume that the source 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. We give new extractors for this model that have exponentially small error, a parameter that is important for an application in cryptography.

The Unique Games Conjecture with Entangled Provers is False

Oded Regev (Tel Aviv University, IL)

We consider one-round games between a classical verifier and two provers who share entanglement. We show 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. Essentially the only algorithm known previously was for the special case of binary answers, as follows from the work of Tsirelson in 1980. Among other things, our result implies that the variant of the unique games conjecture where we allow the provers to share entanglement is false. Our proof is based on a novel 'quantum rounding technique', showing how to take a solution to an SDP and transform it to a strategy for entangled provers.

Keywords: Unique games, entanglement

Joint work of: Kempe, Julia; Regev, Oded; Toner, Ben

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1304

Full Paper:
http://arxiv.org/abs/0710.0655

Average-case Efficient Sorting Circuits

Rüdiger Reischuk (Universität Lübeck, D)

In previous work we have introduced an average case measure for the time complexity of Boolean circuits – that is the delay between feeding the input bits into a circuit and the moment when the results are ready at the output gates – and analysed this complexity measure for prefix computations.

Here we consider the problem to sort large integers that are given in binary notation.

Contrary to a *word comparator sorting circuit* C where a basic computational element, a comparator, is charged with a single time step to compare two elements, in a *bit comparator circuit* C' a comparison of two binary numbers has to be implemented by a Boolean subcircuit CM called *comparator module* that is built from Boolean gates of bounded fanin.

Thus, compared to C, the depth of C' will be larger by a factor up to the depth of CM.

Our goal is to minimize the average delay of bit comparator sorting circuits.

The worst-case delay can be estimated by the depth of the circuit.

For this worst-case measure two topologically quite different designs seems to be appropriate for the comparator modules: a tree-like one if the inputs are long numbers, otherwise a linear array working in a pipelined fashion.

Inserting these into a word comparator circuit we get bit level sorting circuits for binary numbers of length m for which the depth is either increased by a multiplicative factor of order $\log m$ or by an additive term of order m.

We show that this obvious solution can be improved significantly by constructing efficient sorting and merging circuits for the bit model that only suffer a constant factor time loss on the average if the inputs are uniformly distributed.

This is done by designing suitable hybrid architectures of tree compaction and pipelining.

These results can also be extended to classes of nonuniform distributions if we put a bound on the complexity of the distributions themselves.

Keywords: Sorting circuits, average case complexity, circuit delay

Joint work of: Jakoby, Andreas; Liśkiewicz, Maciej; Reischuk, Rüdiger; Schindelhauer, Christian

Infeasibility of Instance Compression and Succinct PCPs for NP

Rahul Santhanam (University of Toronto, CA)

We study the notion of "instance compressibility" of NP problems [Harnik-Naor06], closely related to the notion of kernelization in parameterized complexity theory [Downey-Fellows99, Flum-Grohe06, Niedermeier06]. A language L in NP is instance compressible if there is a polynomial-time computable function f and a set A such that for each instance x of L, $f(x)$ is of size polynomial in the it witness size of x, and f reduces L to A. We prove that SAT is not instance compressible unless NP is contained in coNP/poly, and the Polynomial Hierarchy collapses. This result settles an open problem posed by [Harnik-Naor06] and [Downey07], and has a number of implications: 1. A number of parametric NP problems, including SAT, Clique, DominatingSet and IntegerProgramming, are not polynomially kernelizable unless NP is contained in coNP/poly. 2. SAT does not have "succinct PCPs", i.e., PCPs of size polynomial in the number of variables, unless NP is contained in coNP/poly. 3. An approach of Harnik and Naor to constructing collision-resistant hash functions from one-way functions is inviable in its present form. 4. (Burhman) There are no sub-exponential size complete sets for NP or coNP unless NP is contained in coNP/poly.

Keywords: Instance compression, parametric problems, Polynomial Hierarchy, cryptography, PCPs

Joint work of: Fortnow, Lance; Santhanam, Rahul

Diagonal Circuit Identity Testing and Lower Bounds

Nitin Saxena (CWI - Amsterdam, NL)

In this talk we give a deterministic polynomial time algorithm for testing whether a *diagonal* depth-3 circuit $C(\arg xn)$ (i.e. C is a sum of powers of linear functions) is zero.

Keywords: Arithmetic circuit, identity testing, depth 3, depth 4, determinant, permanent, lower bound

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2008/1308

Learning, Testing and Approximating Halfspaces

Rocco Servedio (Columbia University, USA)

A halfspace is a Boolean function of the form f(x) = sign($w \cdot x - \theta$). Halfspaces (also known as linear threshold functions, weighted majority functions, threshold gates, etc.) are a simple, natural and well-studied class of functions.

We describe recent results on approximating, testing, and learning halfspaces over the Boolean cube $\{+1, -1\}^n$. In more detail,

- Every halfspace can be approximated by a halfspace with small integer weights;
- There is an efficient algorithm for testing whether an unknown Boolean function is a halfspace (versus far from every halfspace);
- Halfspaces can be efficiently approximately reconstructed from approximations to their degree-0 and degree-1 Fourier coefficients (this corresponds to an efficient learning algorithm in the "restricted focus of attention" learning model).

The talk will emphasize the connections between these three results.

The talk is based in part on joint work with K. Matulef, R. Rubinfeld and R. O'Donnell, and with R. O'Donnell.

Keywords: Halfspaces

Low-end uniform hardness versus randomness tradeoffs for AM

Ronen Shaltiel (Haifa University, IL)

In 1998, Impagliazzo and Wigderson proved a hardness vs. randomness tradeoff for BPP in the *uniform setting*, which was subsequently extended to give optimal tradeoffs for the full range of possible hardness assumptions by Trevisan and Vadhan (in a slightly weaker setting). In 2003, Gutfreund, Shaltiel and Ta-Shma proved a uniform hardness vs. randomness tradeoff for AM, but that result only worked on the "high-end' of possible hardness assumptions. In this work, we give uniform hardness vs. randomness tradeoffs for AM that are near-optimal for the full range of possible hardness assumptions. Following Gutfreund et al. we do this by constructing a hitting-set-generator (HSG) for AM with "resilient reconstruction.' Our construction is a recursive variant of the Miltersen-Vinodchandran HSG, the only known HSG construction with this required property. The main new idea is to have the reconstruction procedure operate implicitly and locally on superpolynomially large objects, using tools from PCPs (low-degree testing, self-correction) together with a novel use of extractors that are built from Reed-Muller codes for a sort of locally-computable error-reduction. As a consequence we obtain gap theorems for AM (and AM $\cap$ coAM) that state, roughly, that either AM (or AM $\cap$ coAM) protocols running in time $t(n)$ can simulate all of EXP ("Arthur-Merlin games are powerful'), or else all of AM (or AM $\cap$ coAM) can be simulated in nondeterministic time $s(n)$ ("Arthur-Merlin games can be derandomized'), for a near-optimal relationship between $t(n)$ and $s(n)$. As in the paper of Gutfreund et al., the case of AM $\cap$ coAM yields a particularly clean theorem that is of special interest due to the wide array of cryptographic and other problems that lie in this class.

Keywords: Derandomization, Pseudorandomness, Arthur-Merlin games

Joint work of: Shaltie, Ronen; Umans, Chris

Full Paper:
http://eccc.hpi-web.de/eccc-reports/2007/TR07-069/index.html

Simulating Quantum Correlations with Finite Communication

Ben Toner (CWI - Amsterdam, NL)

Assume Alice and Bob share some bipartite d-dimensional quantum state. As is well known, by performing two-outcome measurements, Alice and Bob can produce correlations that cannot be obtained classically. We show that by using only two bits of communication, Alice and Bob can classically simulate any such

correlations. All previous protocols for exact simulation required the communication to grow to infinity with the dimension d. Our protocol and analysis are based on a power series method, resembling Krivine's bound on Grothendieck's constant, and on the computation of volumes of spherical tetrahedra.

Joint work of: Toner, Ben; Regev, Oded

Full Paper:
http://arxiv.org/abs/0708.0827

Unbalanced Expanders and Randomness Extractors from Parvaresh-Vardy Codes

Christopher Umans (CalTech - Pasadena, USA)

We give an improved explicit construction of highly unbalanced bipartite expander graphs with expansion arbitrarily close to the degree (which is polylogarithmic in the number of vertices). Both the degree and the number of right-hand vertices are polynomially close to optimal, whereas the previous constructions of Ta-Shma, Umans, and Zuckerman (STOC '01) required at least one of these to be quasipolynomial in the optimal. Our expanders have a short and self-contained description and analysis, based on the ideas underlying the recent list-decodable error-correcting codes of Parvaresh and Vardy (FOCS '05).

Our expanders can be interpreted as near-optimal "randomness condensers," that reduce the task of extracting randomness from sources of arbitrary min-entropy rate to extracting randomness from sources of min-entropy rate arbitrarily close to 1, which is a much easier task. Using this connection, we obtain a new construction of randomness extractors that is optimal up to constant factors, while being much simpler than the previous construction of Lu et al. (STOC '03) and improving upon it when the error parameter is small (e.g. 1/poly(n)).

Keywords: Extractors, Expanders, Error-correcting codes

Joint work of: Guruswami, Venkatesan; Umans, Christopher; Vadhan, Salil

Full Paper:
http://www.cs.caltech.edu/∼umans/papers/GUV07.pdf

Noise threshold for universality of 2-input gates

Falk Unger (CWI - Amsterdam, NL)

Evans and Pippenger showed in 1998 that noisy gates with 2 inputs are universal for arbitrary computation (i.e. can compute any function with bounded error), if all gates fail independently with probability epsilon and epsilon<= 8.856

We show that formulas built from gates with 2 inputs, in which each gate fails with probability at least epsilon cannot be universal. Hence, there is a threshold on the tolerable noise for formulas with 2-input gates and it is epsilon. We conjecture that the same threshold also holds for circuits.

Full Paper:
http://homepages.cwi.nl/~unger/FormulaOrNoise_ISIT2007.pdf

An algebraic method in random string selection

Nikolai K. Vereshchagin (Moscow State University, RUS)

We study the two party problem of randomly selecting a string among all the strings of length n. We want the protocol to have the property that the output distribution has high entropy, even when one of the two parties is dishonest and deviates from the protocol. We develop protocols that achieve high, close to n, entropy.

In the literature the randomness guarantee is usually expressed as being close to the uniform distribution or in terms of resiliency.

The notion of entropy is not directly comparable to that of resiliency, but we establish a connection between the two that allows us to compare our protocols with the existing ones.

We construct an explicit protocol that yields entropy $n-O(1)$ and has $4log^*n$ rounds, improving over the protocol of Goldwasser et al. that also achieves this entropy but needs O(n) rounds. Both these protocols need $O(n^2)$ bits of communication.

Next we reduce the communication in our protocols. We show the existence, non-explicitly, of a protocol that has 6-rounds, $2n+8\log n$ bits of communication and yields entropy $n - O(\log n)$ and min-entropy $n/2 - O(logn)$. Our protocol achieves the same entropy bound as the recent, also non-explicit, protocol of Gradwohl et al., however achieves much higher min-entropy: $n/2-O(logn)$ versus $O(logn)$.

Finally we exhibit very simple explicit protocols. We connect the security parameter of these geometric protocols with the well studied Kakeya problem motivated by harmonic analysis and analytical number theory. We are only able to prove that these protocols have entropy 3n/4 but still n/2 - O(log n) min-entropy. Therefore they do not perform as well with respect to the explicit constructions of Gradwohl et al. entropy-wise, but still have much better min-entropy. We conjecture that these simple protocols achieve n -o(n) entropy. Our geometric construction and its relation to the Kakeya problem follows a new and different approach to the random selection problem than any of the previously known protocols.

Keywords: Shannon entropy, Random string ds

Joint work of: Vereshchagin, Nikolai K.; Buhrman, Harry; Cristandl, Matthias; Koucky, Michal; Lotker, Zvi; Patt-Shamir, Boaz

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2008/1309

Directed Planar Reachability is in Unambiguous Logarithmic Space.

N. Variyam Vinodchandran (University of Nebraska, USA)

We show that directed planar reachability problem is in unambiguous logarithmic space (UL).

Keywords: Complexity classes, space bounded computation, reachability problems.

Joint work of: Bourke, Chris; Tewari, Raghunath; Vinodchandran, N. V.

Heuristic approximation of BPTIME[sublinear] with short advice

Marius Zimand (Towson University - Baltimore, USA)

The standard way for non-uniform derandomization of BPTIME[sublinear] (i.e., the "Adleman's trick") establishes that, for every s and t, BPTIME[sublinear] $\subseteq heur_{2^{-s}}\ DTIME[st]/O(st)$. The advice information can be reduced to $t+O(s)$ by using expander-based sampling. We show, that by using exposure-resilient extractors, in the case of sublinear time, the advice information can be further reduced to $O(\log(t) + s)$. More precisely, if $t^{18} \cdot s^9 < n$ and $s = \Omega(\log n)$, BPTIME[t] $\subseteq heur_{2^{-s}}\ DTIME[O(s \cdot t \cdot polylog \cdot (t))]/O(\log t + s)$.

Keywords: Derandomization, sublinear time, extractor

Algebraic Quantum Circuits

Wim van Dam (Univ. California - Santa Barbara, USA)

A model of algebraic quantum circuit computation is introduced for all finite fields GF(q). The wires in this model carry superpositions over the elements of GF(q), and its gates are the Fourier transform over GF(q) and a finite set of controlled phase rotations. The amplitudes of the circuit C can then be expressed as an exponential sum for a multivariate polynomial f_C with integer coefficients. Using earlier work on exponential sums we show that the probabilities of the circuit converge to 0 or to 1 in the limit of large q.

Keywords: Quantum computing, algebraic circuits, exponential sums