Dagstuhl Seminar 02421 on

Algebraic Methods in Quantum and Classical Models of Computation

13.10. - 18.10 2002

organized by

Harry Buhrman (CWI Amsterdam)

Lance Fortnow (NEC Princeton)

Thomas Thierauf (Univ. Ulm/FH Aalen)

Contents

1 Scientific Report

The seminar brought together groups from two research areas: *quantum information processing* and *computational complexity*. Having said that the most important talk of the workshop dealt with neither. Manindra Agrawal gave a presentation on the new primality algorithm he developed with his students. They discovered the first provably deterministic efficient algorithm for determining whether a number is prime. This is the most important theoretical computer science result in at least a decade. We were very lucky at Dagstuhl to have Agrawal give this talk, the first talk he gave on the subject outside of his native India.

Steve Fenner gave the first talk giving a wonderful overview of quantum computation for classical complexity theorists. In addition, Steve Høyer showed how to use quantum algorithm as black box subroutines to create new quantum algorithms. These two talks helped produce the synergy of the two areas for the rest of the conference.

The main theme of the workshop considered algebraic methods in the study of both areas and we had several talks along these lines. Scott Aaronson and Andris Ambainis gave talks showing how polynomials and group representations give lower bounds for quantum machines while Ken Regan described how the algebraic degree can lead to lower bounds in classical complexity. Eldar Fischer showed how Fourier transforms play a role in the recently exciting area of property testing.

The graph isomorphism question, a special case of the hidden subgroup problem, has interest to both classical and quantum theorists. Jacobo Torn and V. Arvind discussed the classical complexity of graph isomorphism while Wim van Dam talked about quantum algorithms for cases of the hidden subgroup problem.

Other quantum talks include work on quantum branching programs (Ablayev), quantum circuits (Fenner, Green, Spalek) and quantum Kolmogorov Complexity (Vitanyi).

In addition to Agrawal's presentation on primality, we had a wide-range of talk on classical complexity. Pierre McKenzie described circuits over sets of natural numbers. He gave an exciting open question that many of the attendees struggled over (unsuccessfully) for many hours during the workshop. Bill Gasarch talked about the cake-cutting problem, how to cut a cake so all are happy with the outcome that had equally intriguing open questions.

Jack Lutz talked about his recent interests in effective Fractal dimension, an extension of his work on resource-bounded measure. Denis Therien

classified the communication complexity for regular languages.

Rounding out the conference were talks on classical subjects by Stephan, Hertrampf, Reischuk, and Miltersen.

2 Public Outreach

In the past fifteen years, we have seen several surprising results in computational complexity based on algebraic techniques. For example Barrington's Theorem showing that majority can be computed by bounded-width branching programs uses noncommutative groups, or the research on interactive proofs and probabilistically checkable proofs that led to hardness of approximability results rely heavily on the structure of the zeros of low-degree polynomials.

Nowhere though has the power of algebra played a larger role than in the study of quantum computation. One can view quantum computation as multiplication of unitary matrices. Shor's famous quantum algorithm for factoring relies heavily on the algebraic structure of the groups Z_m and can be seen as a special case of the hidden subgroup problem for abelian groups. The more general case for non-abelian groups is still a tantalizing open problem and could lead to a polynomial time quantum algorithm for the Graph Isomorphism problem.

Our proposed workshop would bring together leading researchers using algebraic techniques from both the quantum computation area and those studying classical models. Combining these groups of researchers will hopefully lead to a greater understanding of the computational power of both quantum and classical models of computation through new applications of algebraic techniques.

3 Abstracts of Presentations

A Physics-Free Introduction to Quantum Computing

Steve Fenner
University of South Carolina

We present the standard model of quantum computation by analogy with classical deterministic Boolean circuits and with probabilistic circuits. We describe how a simple change of definition leads to all three models. For example, probabilistic gates preserve the l_1 norm and quantum gates preserve the l_2 norm.

Quantum Black Box Algorithms

Peter Hoyer
University of Calgary

We discuss upper and lower bounds in the quantum black box model. We show a lower bound of $O(n^{3/2})$ and an upper bound of $O(n^{7/4})$ for Matrix Multiplication Verification, and tight $\Theta(n^{1/2})$ bound for AND-OR trees.

Infinitely Often Autoreducible Sets

Frank Stephan
Universität Heidelberg

Joint work with Richard Beigel and Lance Fortnow

A set A is autoreducible if one can compute, for all x, the value $A(x)$ with querying A only at places y different from x. Furthermore, A is infinitely often autoreducible if, for infinitely many x, the value $A(x)$ can be computed with querying A only at places y different from x; for all other x, the computation outputs a special symbol to signal that the reduction is undefined. It is shown that for polynomial time Turing and truth-table autoreducibility there are sets A, B, C in EXP such that A is not infinitely often Turing autoreducible, B is Turing autoreducible but not infinitely often truth-table autoreducible, C is truth-table autoreducible with $g(n) + 1$ queries but not infinitely often Turing autoreducible with $g(n)$ queries. Furthermore, connections between notions of infinitely often autoreducibility and notions of approximability are investigated.

Cake Cutting: A new Area for Complexity Theory

Bill Gasarch
University of Maryland at College Park

If 2 people want to cut a cake it is easy to be fair: one cuts, the other choose. What if n people want to cut a cake? Is there a protocol to be fair? What does fair mean?

We define a cutting of the cake to be **proportional** if at the end everyone has at least $1/n$ of the cake. (Note that different people may value different parts of the cake differently). The question now arises

1. Is there a protocol that is fair?

2. How many cuts does it take?

We should that there is a protocol that takes $O(n \log n)$ cuts. We raise the question of whether or not there is an $O(n)$ protocol. There is an easy lower bound of $n-2$ cuts, and a harder one of $n-1$ cuts.

It is possible that even though a cutting is proportional, Alice things Bob got a bigger piece. A cutting is **envy free** if everything thinks they got the biggest piece or were tied for it.

We show that there is an envy-free protocol for $n = 3$. This one takes at most 5 cuts. If you want an envy free protocol for $n = 4$, it exists, but the number of cuts is unbounded. It depends on the preference functions of the individual.

Open Problem 1 Prove an $\Omega(n \log n)$ lower bound on Proportional Cake Cutting,

Open Problem 2 Prove or Disprove that there is a bounded Envy Free Cake Cutting.

We note that all of our algorithms are discrete (not 'moving knife protocols') and that **none** of the work here is ours. See **Fair Division** by Brams and Taylor, or **Cake Cutting: be fair if you can** by Robertson and Webb

Quantum and Stochastic Branching Programs of Bounded Width

Farid Ablayev
Kazan State University

We prove upper and lower bounds on the power of quantum and stochastic branching programs of bounded width. We show any NC^1 language can be accepted exactly by a width-2 quantum branching program of polynomial length, in contrast to the classical case where width 5 is necessary unless NC^1=ACC. This separates width-2 quantum programs from width-2 doubly stochastic programs as we show the latter cannot compute the middle bit of multiplication. Finally, we show that bounded-width quantum and stochastic programs can be simulated by classical programs of larger but bounded width, and thus are in NC^1.

The Complexity of Circuit Evaluation over the Natural Numbers

Pierre McKenzie
Université de Montréal

Joint work with Klaus Wagner

The problem of testing membership in the subset of the natural numbers produced at the output gate of a $\{\cup, \cap, ^-, +, \times\}$ combinational circuit is shown to capture a wide range of complexity classes. Although the general problem remains open, the case $\{\cup, \cap, +, \times\}$ is shown NEXPTIME-complete, the cases $\{\cup, \cap, ^-, \times\}$, $\{\cup, \cap, \times\}$, $\{\cup, \cap, +\}$ are shown PSPACE-complete, the case $\{\cup, +\}$ is shown NP-complete, the case $\{\cap, +\}$ is shown C=L-complete, and several other cases are resolved. Interesting auxiliary problems are sometimes required, such as testing nonemptyness for union-intersection-concatenation circuits, and expressing each integer, drawn from a set given as input, as powers of relatively prime integers of one's choosing. Our results extend in nontrivial ways past work by Stockmeyer and Meyer (1973), Wagner (1984) and Yang (2000).

Quantum Kolmogorov Complexity

Paul Vitányi
CWI Amsterdam

We develop a theory of the algorithmic information in bits contained in an individual pure quantum state. This extends classical Kolmogorov complexity to the quantum domain retaining classical descriptions. Quantum Kolmogorov complexity coincides with the classical Kolmogorov complexity on the classical domain. Quantum Kolmogorov complexity is upper bounded and can be effectively approximated from above under certain conditions. With high probability a quantum object is incompressible. Upper- and lower bounds of the quantum complexity of multiple copies of individual pure quantum states are derived and may shed some light on the no-cloning properties of quantum states. In the quantum situation complexity is not sub-additive. We discuss some relations with "no-cloning" and "approximate cloning" properties. Published as quant-ph/9907035 and in final form as P. Vitányi, Quantum Kolmogorov complexity based on classical descriptions, *IEEE Trans. Inform. Th.*, 47:6(2001), 2464–2479.

A Polynomial Time Algorithm for Primality Testing

Manindra Agrawal
IIT Kanpur

Joint work with Neeraj Kayal and Nitin Saxena

Primality testing is a fundamental problem in computational number theory. A number of efficient algorithms are known for the problem however, they are all probabilistic. It has been a major open problem for last three decades to find a deterministic polynomial time algorithm for the problem. In this talk, we present the first such algorithm.

Algebraic Degree and Connectivity in Lower Bounds

Kenneth W. Regan
State University of NY at Buffalo

We attack the problem of extending Shpilka and Wigderson's near-quadratic lower bounds on depth-3 algebraic formulas for certain arithmetical functions [CCC'99]. We do so for functions like $f(x_1, ..., x_n) = x_1^n + ...x_n^n$ that do not satisfy their condition that the span of the d-th order partial derivatives be exponential. The gradient f' of this function f pulls back a point $q \in C^n$ (with no zero coordinates) into $(n-1)^n$ inverse images. For a depth-3 $\Sigma - \Pi - \Sigma$ (sum of products of sums) formula to compute f, the fan-ins d_i to the multiplication gates $g_1, ..., g_i, ..., g_s$ must satisfy $\prod_{i=1}^{s}(d_i - 1) >= (n-1)^n$. This inequality follows by analyzing how many disjoint connected components the gradients of the multiplication gates can pull back such a point q into. (The talk also explained Strassen's degree method and why techniques based solely on it seem to fail here.)

This obtained inequality still does not prove that the total fan-in $M = \sum_i d_i$, which is taken as the size of the formula, must be $\Omega(n^2)$, as we may have $s = n \log n$ with many d_i small. However, subsequent to the talk, it appears possible that an $\Omega(n^2)$ lower bound can be proved for f—and for any function f whose gradient has exponentially many inverse images, hence high algebraic-geometric degree of the mapping ideal of f. This would follow on (1) discarding multiplication gates of size ϵn so that the leftover formula computes $f - g$ where g has degree ϵn, (2) taking q with co-ordinates N large enough so that $f - g$ still pulls a closed ball B_q of radius N^ϵ about q into $(n-1)^n$ disconnected regions around the original roots of $f - q$, and (3) extending the connectivity argument to the case of pulling back a closed

ball B_q. "Stay tuned..." A positive result would improve both the quality of the Shpilka-Wigderson bounds and the range of functions they apply for.

Effective Fractal Dimension

Jack H. Lutz
Iowa State University

The two most important notions of fractal dimension are *Hausdorff dimension*, developed by Hausdorff (1919), and *packing dimension*, developed by Tricot (1982). Both dimensions have the mathematical advantage of being defined from measures, and both have yielded extensive applications in fractal geometry and dynamical systems. In 2000, the speaker proved a simple characterization of Hausdorff dimension in terms of *gales*, which are betting strategies that generalize martingales. Imposing various computability and complexity constraints on these gales produces a spectrum of effective versions of Hausdorff dimension, including constructive, computable, polynomial-space, polynomial- time, and finite-state dimensions. Work by several investigators has already used these effective dimensions to shed light on a variety of topics in theoretical computer science, including algorithmic information theory, computational complexity, prediction, and data compression. Constructive dimension has also been discretized, assigning a dimension $\dim(x)$ to each string $x \in \{0,1\}^*$ in a way that arises naturally from Hausdorff and constructive dimensions and gives the unexpected characterization $K(x) = |x|\dim(x) \pm O(1)$ of Kolmogorov complexity. We survey these developments, along with a very recent result by Hitchcock, Mayordomo and the speaker showing that packing dimension – previously thought to be much more complex than Hausdorff dimension – admits a gale characterization that is an exact dual of that of Hausdorff dimension.

References

[1] J. H. Lutz. Dimension in complexity classes. In *Proceedings of the 15th Annual IEEE Conference on Computational Complexity*, pages 158–169, 2000. Updated version appears as ACM Computing Research Repository Technical Report cs.CC/0203016, 2002.

[2] J. H. Lutz. The dimensions of individual strings and sequences. *Information and Computation*. To appear. Available as ACM Computing Research Repository Technical Report cs.CC/0203017, 2002.

[3] J. M. Hitchcock, J. H. Lutz, and E. Mayordomo. Effective strong dimension with applications to information and complexity. Submitted.

Junta Testing using Fourier Analysis

Eldar Fischer
Technion - Israel Institute of Technology, Haifa

Joint work with Guy Kindler, Dana Ron, Shmuel Safra and Alex Samorodnitsky

Property testing is a rapidly-evolving field that deals with the analysis of algorithms that base their answers on reading only a small portion of their input. Such algorithms cannot be accurate, but in many cases they can distinguish between inputs that satisfy a given property, and inputs that are epsilon-far (where the distance is measured by the Hamming norm) from any input that satisfies the property.

In our case the input is a boolean function with n variables, and the required property is that of depending on only k of the variables. It is possible to test for this property using only poly(k)/epsilon queries to the input. The constructed algorithm is combinatorial in nature, but its analysis relies crucially on a tight connection between the dependency of a function on a set of variables, and a corresponding sum of the squares of some of its Fourier coefficients.

Simulations of Constant Depth Quantum Circuits

Steve Fenner
University of South Carolina

We clarify and strengthen results suggested by DiVincenzo and Terhal regarding simulations of constant depth quantum circuits. We show that if exact sampling simulations of depth 4 circits exist in polynomial time, then coC=P = NP, which implies PH is contained in AM, and hence PH = Σ_2^p.

The complexity of Graph Isomorphism

Jacobo Torán
Universität Ulm

The graph isomorphism problem GI consists in deciding whether there is a bijection between the nodes of two given graphs preserving the edge relation. A major source of interest in GI has been the evidence that this problem is not known to be neither in P nor NP-complete. In fact, there is a common believe that GI does not contain enough structure or redundancy to be hard for NP. In this talk we present several results improving the existing hardness results for GI thus indicating that the problem actually contains more internal structure than expected. First we show that the general GI problem is hard for any logarithmic-space complexity class related to counting. We then prove that the graph isomorphism problem restricted to colored graphs with color multiplicities 2 and 3 is many-one complete for symmetric logarithmic space SL under many-one reductions. These are the strongest hardness and completeness results known for the problem.

Algebraic Acceptance Criteria for Polynomial Time Machines

Ulrich Hertrampf
Universität Stuttgart

We investigate the power of polynomial time machines whose acceptance behaviour is defined by finite groups. The machines output a group element on every computation path, and the input is considered to be accepted, if the product of all these group elements (in a given order determined by the machine) evaluates to one.

It is well known that in this setting cyclic groups lead to so-called MOD-classes (in this case co$\mathrm{MOD}_k\mathrm{P}$ for the cyclic group with k elements) and that non-solvable groups lead to the class PSPACE.

We give lower and upper bounds for abelian and nonabelian solvable groups.

The Future of Quantum Lower Bounds by Polynomials

Scott Aaronson
University of California at Berkeley

The polynomial method is one of the principal known techniques for proving lower bounds on the query complexity of quantum algorithms. In this talk I'll first show how the polynomial method is used to obtain lower bounds for the collision and set comparison problems, and then survey some open problems.

Given a function $f : \{1...n\} \to \{1...n\}$, the collision problem is to decide whether f is 1-to-1 or 2-to-1, given that one of these is the case. We show a lower bound of $\Omega(n^{1/5})$ on the bounded-error quantum query complexity of this problem; previously, no lower bound better than $\Omega(1)$ was known. Also, given $f, g : \{1...n\} \to \{1...2n\}$, the set comparison problem is to decide whether Range(f)=Range(g) or the union of Range(f) and Range(g) has size at least $1.1n$, given that one of these is the case. We show a lower bound of $\Omega(n^{1/7})$ for this problem. A corollary is that there exists an oracle relative to which SZK is not contained in BQP.

Small Constant Depth Quantum Circuits

Fred Green
Clark University

Constant depth quantum circuits can be defined to contain Toffoli gates and arbitrary single-qubit gates. By analogy with the classical counterpart AC^0, we refer to the class of such circuit families (with a fixed number of single-qubit gates per family) as QAC^0. Since AC^0 circuits allow unbounded fanout as well as fanin, it also is natural to define the class QAC^0 With Fanout gates, which we denote $QAC^0_w f$. Surprisingly, these fanout gates add great power to QAC^0. The class $QAC^0_w f$ contains all of classical ACC (in which we allow arbitrary Mod_m gates). Indeed, in the quantum setting any MOD_m gate is as good as any other, up to polynomial size and constant depth, and quantum MOD_2 gates are equivalent to the fanout gate. Thus whereas classically (by a theorem of Smolensky) ACC[p] is not equal to ACC[q] for any pair of distinct primes q and p (and thus ACC[q] is strictly contained in ACC), in the quantum case we have for all m that QACC = QACC[m] = $QAC^0_w f$. While techniques have been developed to prove upper bounds on QACC, it is possible that these classes are even more powerful than expected. For example, by a recent result of Terhal and DiVincenzo, if a nondeterministic language class based on QACC (called NQACC) is in NP, then the polynomial hierarchy collapses to its second level. Most of this work was reported in "Counting, Fanout and the Complexity of Quantum ACC"

by F. Green, S. Homer, C. Moore and C. Pollett in Quantum Information and Computation 2 (2002), pp. 35 - 65.

Quantum Circuits with Unbounded Fan-out

Robert Spalek
CWI Amsterdam

We propose a new circuit class QNCf^0 – constant-depth quantum circuits with unbounded fan-out. It differs from QNC^0 by including the quantum fan-out gate, and from QACC^0 by excluding the Toffoli (AND) gate.

We describe an efficient method for performing commuting gates in parallel. Using this method, we construct approximate circuits for the Counting and linear Threshold gate. Let us assume the weights of the source qubits in the linear combination are bounded by a polynomial $p(n)$. Then both circuits have depth $O(\log\log n + \log\log(1/\epsilon))$ and size $O(\log n(n + \log(1/\epsilon)))$ with error bounded by epsilon.

Furthermore, we construct exact and shallower circuits for these gates at the cost of bigger space complexity. They all have depth $O(\log^* n)$ in the model QNCf, and constant depth in the model QACC. We first define a linear Value gate (testing a linear equation on source qubits) and construct an exact circuit of size $O(n \log n)$ for it. Using this gate, we construct circuits for the Counting and linear Threshold gate of size $O(n^2 p(n) log n)$.

It follows, that $\mathrm{QTCf}^0 = \mathrm{QACC}^0$.

Efficient Quantum Algorithms for Estimating Gauss Sums

Wim van Dam
University of California at Berkeley
Joint work with Gadiel Seroussi

We present an efficient quantum algorithm for estimating Gauss sums over finite fields and finite rings. This is a natural problem as the description of a Gauss sum can be done without reference to a black box function. With a reduction from the discrete logarithm problem to Gauss sum estimation we also give evidence that this problem is hard for classical algorithms. The workings of the quantum algorithm rely on the interaction between the additive characters of the Fourier transform and the multiplicative characters of the Gauss sum.

Communication Complexity of Regular Languages

Denis Therien
McGill University

In this work, we determine the communication complexity of every regular language with a neutral letter in the two party deterministic model, simultaneous model and randomized model. In each case, we show the existence of gaps and the characterization of each complexity class is given using decidable algebraic conditions.

The Intractability of Computing the Hamming Distance to Simple Languages

Rüdiger Reischuk
Universität zu Lübeck

Joint work with Bodo Manthey

Given a language L, the *Hamming distance* of a string x to L is the minimum Hamming distance of x to any string y of length $|x|$ in L, that is the number of positions i where x_i and y_i differ. If, for example, the input data may contain errors this notion becomes important for reliable computations. The *edit distance* between 2 strings is a generalized measure where in addition symbols may be inserted or deleted. It has been shown recently that determining the edit distance of a string to a language is $\mathcal{NP}$-hard even for simple languages in $\mathcal{P}$.

We prove that the Hamming distance to certain languages in $\mathcal{AC}^0$ is hard to approximate: it cannot be approximated within a factor of $O(n^{1/3-\epsilon})$, for any $\epsilon > 0$, unless $\mathcal{P} = \mathcal{NP}$. By reductions between the Hamming and the edit distance this result translates into a nonapproximabilty lower bound of $O(n^{1/6-\epsilon})$ for the edit distance.

Furthermore, the parameterised complexity of computing the Hamming distance to a language is investigated. We prove that for every $t \in \mathbb{N}$ there exists a language in $\mathcal{AC}^0$ such that this problem is $W[t]$-hard, the t-th level of the parameterised complexity hierarchy. Moreover, one can find a language in $\mathcal{P}$ for which this problem becomes even $W[\mathcal{P}]$-hard.

Group Representations and Quantum Computation

Andris Ambainis
University of Letvia

The first part is joint work with Leonard Schulman and UMesh Vazirani (STOC'00)

The talk will describe applications of representation theory of symmetric group to quantum computation. The first application will be computing with highly mixed states. This is a model motivated by experiments in NMR (nucleo-magnetic resonance) implementations of quantum computing. The main difference between theory of quantum computing and NMR is the starting state. In theory, we can prepare the starting state. In NMR, the computation starts in a highly random (mixed) state. We look at the model where the highly random state consists of one perfectly prepared quantum bit and n-1 completely random quantum bits. We show that there is any general transformation from quantum algorithms in the standard theoretical model to one-qubit model must involve an exponential increase in the number of qubits. This indicates that the one-qubit model might be less powerful than general quantum computation. The proof is by reduction to a geometric problem about subspaces which is then solved using representations of symmetric group.

The second application is to quantum fingerprints. Quantum fingerprints are small-dimensional nearly orthogonal states. They are useful in quantum communication and cryptography. We show that existing constructions of quantum fingerprints have some interesting group properties. We then generalize these constructions and show that it is possible to fingerprint any Abelian group but not the symmetric group. We also discuss a link between our negative result on fingerprints for symmetric group and hidden subgroup problem which is an important open problem in quantum computing.

Graph Isomorphism is in SPP

V. Arvind
The Institute of Mathematical Sciences, C.I.T. Campus, Chennai

We show that Graph Isomorphism is in the complexity class SPP, and hence it is in ParityP (in fact, it is in $\mathrm{Mod}_k\mathrm{P}$ for each $k > 1$. We derive this result as a corollary of a more general result: we show that a generic problem FINDGROUP has an FP^{SPP} algorithm.

This general result has other consequences: for example, it follows that the hidden subgroup problem for permutation groups, studied in the context of quantum algorithms, has an FP^{SPP} algorithm. Also, some other algorithmic problems over permutation groups known to be at least as hard as Graph Isomorphism (e.g. coset intersection) are in SPP, and thus in $\mathrm{Mod}_k\mathrm{P}$ for $k > 1$.

Circuits on Cylinders

Peter Bro Miltersen
University of Aarhus

Joint work with Kristoffer Arnsfelt Hansen and V Vinay

We consider the computational power of circuits and branching programs embedded on cylinders. We show that every problem solved by a $\Pi_2 \circ \mathrm{MOD} \circ \mathrm{AC}^0$ circuit can also be solved by a constant width polynomial size cylindrical branching program (or circuit) and that every constant width polynomial size cylindrical circuit can be simulated in ACC^0.