04421 Abstracts Collection
Algebraic Methods in Computational Complexity
— Dagstuhl Seminar —

Harry Buhrman, Lance Fortnow, Thomas Thierauf

[1] CWI - Centrum voor Wiskunde en Informatica
Kruislaan 413, NL-1090 GB Amsterdam, Netherlands
harry.buhrman@cwi.nl
[2] University of Chicago, Dept. of Computer Science
1100 East 58th Street, Chicago, USA
fortnow@cs.uchicago.edu
[3] Fachhochschule Aalen
Beethovenstraße 1, 73430 Aalen, Germany
Thomas.Thierauf@FH-Aalen.de

Abstract. From 10.10.04 to 15.10.04, the Dagstuhl Seminar 04421 "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, algebraic methods, quantum computations, lower bounds.

04421 Summary – Algebraic Methods in Computational Complexity

The seminar brought together 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 saw a series of presentations by Andris Ambainis, Robert Spalek and Mario Szegedy. Ambainis described his improved method for showing lower bounds for quantum algorithms that provably beats the degree method. Spalek talked about his work with Szegedy showing that Ambainis techniques as well as different tools developed by Zhang, Laplante and Magniez, and Barnum, Saks and Szegedy all gave the same bounds. Szegedy, in his presentation, called this complexity measure sumPI and showed that the size of a Boolean formula computing

a function f is at least $\mathsf{sumPI}^2(f)$. Further talks on quantum complexity considered lower bounds for formula size (Scott Aaronson), finite groups (Steve Fenner), and adversary bounds (Robert Spalek).

Discussions between Laplante, Lee and Szegedy at the workshop led to the recent announcement of even a stronger lower bound for Boolean formula complexity using a stronger version of sumPI complexity called maxPI.

Manindra Agrawal presented recent work of his students Neeraj Kayal and Nitin Saxena (the trio that showed a polynomial-time algorithm for primality testing) on rings given by a matrix describing the actions on the base elements. They show a randomized reduction from graph isomorphism to ring isomorphism and from factoring to #RI, counting the number of ring isomorphisms. They also show a polynomial-time algorithm for determining if there are any non-trivial automorphisms of a ring and that #RI is computable with an oracle for $\mathsf{AM} \cap \mathsf{coAM}$. Agrawal conjectured that #RI is computable in polynomial time, a conjecture that would imply factoring and graph isomorphism have efficient algorithms.

In addition to Agrawal's presentation on ring isomorphism, we had a wide-range of talks on classical complexity. Lance Fortnow, building on work of Shaltiel and Umans, characterized the interesting question whether EXP is contained in NP with logarithmically bounded advice. Judy Goldsmith showed that the dominance problem for user preferences is PSPACE-complete. Various hypothesis in complexity theory were compared by John Hitchcock. Jörg Rothe located the Exact-Four-Colorability problem in the boolean hierarchy. Several probabilistic time classes were separated by Rahul Santhanam. Leen Torenvliet considered autoreducible sets and Falk Unger presented some new results on sparse self-reducible sets. Talks on circuit complexity were given by Anna Gal, Ryan O'Donnell and Denis Therien.

Troy Lee considered the symmetry of information in Kolmogorov complexity. Klaus Ambos-Spies presented algorithmic and resource-bounded genericity concepts. Tolerant property tester were investigated by Eldar Fischer, and automatic structures by Frank Stephan. Markus Maucher presented a very interesting relationship between the entropy of random source and the running time of (randomized) quicksort, where the random source is used for the choice of the pivot element. Rüdiger Reischuk considered string compression based on context-free grammars: the problem to determine the minimal size of a grammar that produces precisely one given string x was shown to be NP-hard for alphabets of larger size.

Joint work of: Buhrman, Harry; Fortnow, Lance; Thierauf, Thomas

Formula Size Lower Bounds and Quantum States

Scott Aaronson (IAS - Princeton)

I'll show an explicit exponential lower bound for a Boolean function complexity measure that I call "manifestly orthogonal formula size." The motivation originally came from quantum computing (specifically, from a paper of mine called "Multilinear Formulas and Skepticism of Quantum Computing"), but the lower bound should be of independent interest for classical complexity theory.

The Ring Isomorphism Problem

Manindra Agrawal (Indian Inst. of Technology - Kanpur)

We define and study the complexity of testing if two finite commutative rings are isomorphic. We show that the problem has low complexity (it is in $\mathsf{NP} \cap \mathsf{coAM}$), yet is harder than Graph Isomorphism and Factoring, two well-known problems of intermediate compelxity.

We also show that the related problem of testing if a ring has a non-trivial automorphism is in P.

Polynomial Degree vs.Quantum Query Complexity

Andris Ambainis (University of Waterloo)

We consider computing a Boolean function f by a quantum query algorithm (a quantum counterpart of a decision tree). The degree of a polynomial representing (or approximating) f is a well known lower bound on the number of queries needed by a quantum algorithm. We present the first example where this bound is not tight. Namely, we construct a function with polynomial degree 2^d and quantum query complexity $\Omega(2.5^d)$. To prove the lower bound on the quantum complexity, we use a new weighted version of the quantum adversary method.

Finite State Genericity

Klaus Ambos-Spies (Universität Heidelberg)

Algorithmic and resource-bounded genericity concepts have become elegant and powerful tools in computability and computational complexity theory. Here we explore the power of genericity concepts in the setting of formal language theory focusing on the class of regular languages. We introduce and investigate various genericity concepts based on extension functions computable by finite automata. For bounded finite-state genericity, which is based on extension functions of constant length, we show that the corresponding generic languages are not regular

but can be context-free. Moreover, we give a combinatorical characterization of this concept by showing that a language is bounded finite-state generic if and only if its characteristic sequence is disjunctive (i.e., every binary word occurs in the characteristic sequence as a subword). By considering finite-state extensions of non-constant length we obtain stronger finite-state genericity notions forcing some more fundamental fi! nite-state properties. E.g., for genericity based on generalized Moore functions, the corresponding generic languages are bi-immune to the class of regular languages.

Keywords: Genericity, regular languages, finite automata, disjunctive sequences

Joint work of: Ambos-Spies, Klaus; Busse, Edgar

Quantum algorithms for a set of group theoretic problems

Stephen A. Fenner (University of South Carolina)

We study a set of group theoretic problems over solvable groups, including Group Intersection, Coset Intersection and Double-Coset Membership. We show that there exist efficient quantum algorithms for Group Intersection if one of the underlying groups has a smoothly solvable commutator subgroup, and for Coset Intersection and Double-Coset Membership if one of the underlying groups is smoothly solvable. We also give a reduction from Solvable Group Intersection to the problem Orbit Superposition.

Keywords: Quantum computation, quantum algorithms, group theoretic algorithms, solvable groups, smoothly solvable groups, group intersection, orbit superposition

Joint work of: Fenner, Stephen A.; Zhang, Yong

Tolerant versus intolerant testing for boolean properties

Eldar Fischer (Technion - Haifa)

A recent work of Parnas, Ron and Samorodnitsky introduces the new notion of tolerant testing to the field of property testing. In essence, a property tester (in the strict sense) is a randomized algorithm that reads the input in a number of places that depends only on the approximation parameter ϵ, and distinguishes with probability $2/3$ between the case that the input satisfies a given property, and the case that the input is ϵ-far from satisfying it (in the Hamming distance).

A tolerant tester is a property tester, but one that in addition distinguishes with high probability between inputs that are ϵ-far from satisfying the property, and inputs that are δ-close to satisfying it, where δ also depends only on the approximation parameter ϵ.

For non-Boolean properties it is relatively easy to see that some properties admit a property tester (by the above strict definition), but do not admit a tolerant property tester. The subject of the talk is the construction of a property of Boolean functions that admits a tester, but not a tolerant one. The construction borrows some ideas used in the field of Probabilistically Checkable Proofs, as well as results from the very beginning of the field of property testing, reaffirming the common heritage of the two fields.

Keywords: Property testing, Boolean functions, Hadamard codes.

Joint work of: Fischer, Eldar; Fortnow, Lance

NP with Small Advice

Lance Fortnow (University of Chicago)

Shaltiel and Umans recently showed that $\mathsf{EXP} \in \mathsf{P}_{||}^{\mathsf{NP}}$ implies $\mathsf{EXP} \in \mathsf{NP/poly}$. We strengthen this result and prove a converse:

$\mathsf{EXP} \in \mathsf{P}_{||}^{\mathsf{NP}}$ if and only if $\mathsf{EXP} \in \mathsf{NP}/\log$.

This is joint work with Adam Klivans at TTI-Chicago.

Joint work of: Fortnow, Lance; Klivans, Adam

On the correlation between parity and modular polynomials

Anna Gal (Univ. of Texas at Austin)

We consider the problem of bounding the correlation between parity and modular polynomials modulo q, for arbitrary odd integers q at least 3.

We prove exponentially small upper bounds for classes of polynomials with certain linear algebraic properties. Some of these classes include even polynomials of a certain form with large degree and large number of terms.

As a corollary, we obtain exponential lower bounds on the size necessary to compute parity by depth-3 circuits with a Majority-gate at the top, Mod_q-gates at the middle level and And gates at the input level; when the polynomials corresponding to the depth-2 Mod_q-And-subcircuits satisfy our conditions.

Our methods also yield lower bounds for depth-3 Maj-Mod_q-Mod_2-circuits (under certain restrictions) for computing parity.

Our technique is based on a new general representation of the correlation using exponential sums, that takes advantage of the linear algebraic structure of the corresponding polynomials.

Joint work of: Gal, Anna; Trifonov, Vladimir

Constructing Large Subsets of $[n]$ Without Arithmetic Progressions of Length Three

William Gasarch (University of Maryland)

Given n, what is the largest subset of $[n]$ that does not have any arithmetic progresion of length three? We will first show two applications of these types of results to complexity theory (one in Comm Complexity, one in PCP). We then survey the literature for constructions of such sets. Lastly we introduce some modifications to the literture which yield bigger sets in practice

Keywords: PCP, Communication Complexity, Arithmetic Sequence,

Joint work of: Gasarch, William; Glenn, James

The communication complexity of the Exact-N Problem revisited

William Gasarch (University of Maryland)

If Alice has x, y, Bob has x, z and Carol has y, z can they determine if $x+y+z = N$? They can if (say) Alice broadcasts x to Bob and Carol; can they do better? Chandra, Furst, and Lipton studied this problem and showed sublinear upper bounds.

They also had matching (up to an additive constant) lower bounds. We give an exposition of their result with some attention to what happens for particular values of N.

Keywords: Communication Complexity, Exact-N problem, Arithmetic Sequences

Joint work of: Gasarch, William; Glenn, James; Utis, Andre

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2005/102

Preferences and Domination

Judy Goldsmith (University of Kentucky)

CP-nets are a succinct formalism for specifying preferences over a multi-featured domain. A CP-net consists of a directed graph, with nodes representing the features of the domain, and edges indicating conditional preferences.

An instance in the domain is an assignment of values to the features. An instance alpha is preferred to an instance beta if there are a sequence of "improving flips" from alpha to beta, where an improving flip changes the value of one feature to a more-preferred value, based on the values of the parents of that feature. We say alpha dominates beta if such a sequence exists.

We show that recognizing dominance is PSPACE hard for cyclic CP-nets.

Keywords: Preferences, CP-nets, PSPACE-complete, reductions

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2005/103

Hardness Hypotheses, Derandomization, and Circuit Complexity

John M. Hitchcock (University of Wyoming)

We consider three complexity-theoretic hypotheses that have been studied in different contexts and shown to have many plausible consequences.

- The measure hypothesis: NP does not have p-measure 0.
- The pseudo-NP hypothesis: there is an NP language L such that any DTIME(2^{n^e}) language L' can be distinguished from L by an NP refuter.
- The NP-machine hypothesis: there is an NP machine accepting 0^* for which no 2^{n^e}-time machine can find infinitely many accepting computations.

We show that the NP-machine hypothesis is implied by each of the first two. Previously, no relationships were known among these three hypotheses. Moreover, we unify previous work by showing that several derandomizations and circuit-size lower bounds that are known to follow from the first two hypotheses also follow from the NP-machine hypothesis. We also consider UP versions of the above hypotheses as well as related immunity and scaled dimension hypotheses.

Joint work of: Hitchcock, John M.; Pavan, A.

Resource Bounded Symmetry of Information

Troy Lee (CWI - Amsterdam)

The principle of symmetry of information, which states $C(x,y) = C(x)+C(y|x)$, is very useful and beautiful theorem in Kolmogorov complexity. We investigate if an analogue of this theorem holds when resource restrictions are placed on the programs which print a string x from its description. We are especially interested in programs using nondeterminism and randomness.

For nondeterministic programs, we show an oracle where symmetry of information fails in a strong way: we show there is an oracle A such that $(2-\epsilon)CN^A(x,y) < CN^A(x) + CN^A(y|x)$, where $CN(y|x)$ is the length of a shortest nondeterministic program which prints y given x.

On the other hand, for nondeterministic programs with randomness, we show $C^p(x,y) > CAM(x) + CAM(y|x) - O(log^3|x| + |y|)$.

This last statement implies symmetry of information holds under the assumption $C^p(x|y) < CAM(x|y)$. We show, however, that this assumption implies P = NP.

Joint work of: Lee, Troy; Romashchenko, Andrei

Randomized QuickSort and the Entropy of the Random Source

Markus Maucher (Universität Ulm)

The worst-case complexity of an implementation of Quicksort depends on the random number generator that is used to select the pivot elements. In this paper we estimate the expected number of comparisons of Quicksort as a function in the entropy of the random source. We give upper and lower bounds and show that the expected number of comparisons increases from $n \log n$ to n^2, if the entropy of the random source is bounded. As examples we show explicit bounds for distributions with bounded min-entropy and the geometrical distribution.

Keywords: Randomized Algorithms, QuickSort, Entropy

Joint work of: List, Beatrice; Maucher, Markus; Schöning, Uwe; Schuler, Rainer

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2005/104

Polynomial Threshold Functions

Ryan O'Donnell (Microsoft Research - Seattle)

The "PTF (Polynomial Threshold Function) problem" is the following:

Let $S_1, \ldots, S_m$ be some disjoint regions in R^n, each labeled by a sign, either $-$ or $+$. What is the lowest possible degree of an n-variate polynomial which is positive on the regions labeled $+$ and negative on the regions labeled $-$?

I will talk about the PTF problem and its relevance to complexity theory. By way of illustrating the many interesting ideas involved, I will give a proof of the Beigel-Reingold-Spielman theorem: PP is closed under intersection.

On the Complexity of Optimal Grammar-based Compression

Rüdiger Reischuk (Universität Lübeck)

Grammar-based compression is a structural approach to compress strings by textual substitution, a field pioneered by Lempel and Ziv with methods based on dictionaries.

Given a string x over some alphabet, the task is to construct a context-free grammar G_x that generates x as the only terminal string.

The question arises what is the minimal size of such a grammar and how can it generated efficiently? This problem has shown to be NP-hard for alphabets of larger size.

To reduce a large alphabet to a smaller one a standard method is to use blockcodes.

We investigate the relation between grammar-based compression of strings and their codewords for such codes.

The minimal grammar size of a codeword is compared to the minimal grammar size of the original string and vice versa by establishing asymptotically tight bounds. One can construct examples where smaller alphabets may allow a substantial more compact coding.

On the other hand, it is shown that for special blockcodes the difference can be at most a small linear factor.

From this we can also deduce a relation between different alphabet sizes concerning approximability.

If there exists a polynomial time factor c-approximation algorithm for the Minimum Grammar Compression problem restricted to binary strings, then there exists a polynomial time factor $(24c + o(1))$-approximation algorithm for the general Minimum Grammar Compression problem over arbitrary alphabets. These results may help in solving the long standing open problem to determine the complexity of the Minimum Grammar Compression problem for binary alphabets.

Keywords: Compression, Formal Grammar, approximability

Joint work of: Arpe, Jan; Reischuk, Rüdiger

Exact-Four-Colorability, Exact Domatic Number Problems, and the Boolean Hierarchy

Jörg Rothe (Universität Düsseldorf)

This talk surveys some of the work that was inspired by Wagner's general technique to prove completeness in the levels of the boolean hierarchy over NP. In particular, we show that it is DP-complete to decide whether or not a given graph can be colored with exactly four colors. DP is the second level of the boolean hierarchy. This result solves a question raised by Wagner in his 1987 TCS paper; its proof uses a clever reduction by Guruswami and Khanna.

Similar results on various versions of the exact domatic number problem are also discussed.

The result on Exact-Four-Colorability appeared in IPL, 2003. The results on exact domatic number problems, obtained jointly with Tobias Riege, are to appear in TOCS.

Keywords: Exact Colorability, exact domatic number, boolean hierarchy completeness

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2005/105

Hierarchy Theorems for Probabilistic Polynomial Time

Rahul Santhanam (University of Chicago)

We show -

1. For each r, there is a language computable in BPP with 1 bit of advice but not in $\mathsf{BPTIME}(n^r)$ with 1 bit of advice
2. For each r, there is a language computable on average in BPP but not on average in $\mathsf{BPTIME}(n^r)$

Joint work of: Fortnow, Lance; Santhanam, Rahul

All Quantum Adversary Bounds are Equivalent

Robert Spalek (CWI - Amsterdam)

The quantum adversary method is one of the most versatile lower-bound methods for quantum algorithms. We show that all known variants of this method are equal up to a multiplicative factor: weighted adversary [Amb03], strong weighted adversary [Zha04], spectral adversary [BSS03], and the Kolmogorov complexity adversary [LM04]. We also present a few new equivalent formulations of the method. This shows that there is essentially *one* quantum adversary method.

From our approach, all known limitations of all versions of the quantum adversary method easily follow.

Keywords: Quantum computing, lower bounds, quantum adversary

Joint work of: Spalek, Robert; Szegedy, Mario

See also: http://arxiv.org/abs/quant-ph/0409116

Automatic Structures

Frank Stephan (National University of Singapore)

Automatic structures are algebraic strutures which are represented in a way that the domain and the relations considered are recognizable by finite automata.

The author gave a summary of results obtained togethe with Bakhadyr Khoussainoiv, Andre Nies and Sasha Rubin.

These results include: Every automatic tree with an infinite branch has also a regular infinite branch.

Every automatic tree with at most countably many infinite branches has only regular branches.

The Finite Condensation rank of an automatic linear ordering is finite.

This permits an alternative proof for De Homme's result that the well-ordered set defined by an ordinal is automatic iff this ordinal is bounded by some power ω^n where n is a natural number.

The additive groups of the integers and the dyadic numbers are automatic, but it is an open problem whether the additive group of the rationals has an automatic presentation.

Furthermore, some negative results were given:

The random graph has no automatic presentation.

No infinite integral domain and no infinite field has an automatic presentation.

Every automatic Boolean Algebra has an atom.

The multiplicative semigroup of the natural numbers does not have an automatic presentation, the same holds for every semigroup containing this semigroup as a subset.

Keywords: Automatic structures; finite automata; trees; groups; random graph

Finding Isolated Cliques by Queries – An Approach to Fault Diagnosis with Many Faults

Frank Stephan (National University of Singapore)

A well-studied problem in fault diagnosis is to identify the set of all good processors in a given set $\{p_1, p_2, \ldots, p_n\}$ of processors via asking some processors p_i to test whether processor p_j is good or faulty. Mathematically, the set C of the indices of good processors forms an isolated clique in the graph with the edges $E = \{(i,j) :$ if you ask p_i to test p_j then p_i states that "p_j is good"$\}$; where C is an isolated clique iff it holds for every $i \in C$ and $j \neq i$ that $(i,j) \in E$ iff $j \in C$.

In the present work, the classical setting of fault diagnosis is modified by no longer requiring that C contains at least $\frac{n+1}{2}$ of the n nodes of the graph. Instead, one is given a lower bound a on the size of C and the number n of nodes and one has to find a list of up to n/a candidates containing all isolated cliques of size a or more where the number of queries whether a given edge is in E is as small as possible.

It is shown that the number of queries necessary differs at most by n for the case of directed and undirected graphs. Furthermore, for directed graphs the lower bound $n^2/(2a-2) - 3n$ and the upper bound $2n^2/a$ are established. For some constant values of a, better bounds are given. In the case of parallel queries, the number of rounds is at least $n/(a-1) - 6$ and at most $O(\log(a)n/a)$.

Keywords: Isolated Cliques, Query-Complexity, Fault Diagnosis

Joint work of: Gasarch, William; Stephan, Frank

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2005/106

The quantum adversary method and formula size lower bounds

Mario Szegedy (Rutgers Univ. - Piscataway)

We introduce two new complexity measures for Boolean functions, or more generally for functions of the form $f : S \to T$, where $S \subseteq \Sigma^n$ for some alphabet Σ and T an arbitrary set. We call these measures sumPI and maxPI. The quantity sumPI has been emerging through a line of research on quantum query complexity lower bounds via the so called quantum adversary method, culminating in [SS04] with the realization that these many different formulations are in fact equivalent. Given that sumPI turns out to be such a robust invariant of a function, we begin to investigate this quantity in its own right and see that it also has applications to classical complexity theory.

As a surprising application we show that $\mathsf{sumPI}^2(f)$ is a lower bound on the formula size, and even, up to a constant multiplicative factor, the probabilistic formula size of f. We show that several formula size lower bounds in the literature, including Khrapchenko [K71] and its extensions [Kou93] are in fact special cases of our method.

The second quantity we introduce, $\mathsf{maxPI}(f)$, is always at least as large as $\mathsf{sumPI}(f)$, and is derived from sumPI in such a way that $\mathsf{maxPI}^2(f)$ remains a lower bound on formula size.

While $\mathsf{sumPI}(f)$ is always a lower bound on the quantum query complexity of f this is not the case in general for $\mathsf{maxPI}(f)$.

A strong advantage of $\mathsf{sumPI}(f)$ is that it has both primal and dual characterizations, and thus it is relatively easy to give both upper and lower bounds on the sumPI complexity of functions.

To demonstrate this, we look at a few concrete examples. We characterize the sumPI complexity of the height h recursive majority of three function, which immediately gives a bound of 2^h for the bounded error quantum query complexity, and 4^h for the probabilistic formula size. We also characterize the *spi* complexity of a function defined by Ambainis [A03] and show that for this function our method gives a much stronger lower bound on the formula size than is possible with Khrapchenko's method. Finally, we show that for partial functions the quantity maxPI can be much larger than sumPI.

Keywords: Quantum computing formula size quantum adversary method Khrapchenko bound

Joint work of: Sophie Laplante, Troy Lee, Mario Szegedy

New upper and lower bounds on the circuit complexity of some regular languages

Denis Therien (McGill University - Montreal)

We characterize the class of regular languages which can be recognized by AC^0 circuits using a linear number of wires. We are also able to exhibit a regular language which can be done in ACC^0 with a linear number of gates but not with a linear number of wires. It is not clear if the same holds for AC^0.

Joint work of: Koucky, Michal; Pudlak, Pavel and Therien, Denis

Using structural properties to separate complexity classes

Leen Torenvliet (University of Amsterdam)

For many pairs of complexity classes A and B, e.g., P and NP, P and PSPACE, NP and EXP, the relation is still unclear many years after their definition. All is fair in the game of separation, and any effort is justified by the goal. For the past ten years, initiated by Harry Buhrman and in cooperation with Lance Fortnow, Albrecht Hoene, Dieter van Melkebeek and recently Stuart Kurtz, we have been investigating the following approach. First we define some structural property P. Next we demonstrate that class A has the property and that B does not have it. This then proves that A is not B.

The approach is not new and dates back to a similar program by Post started 1944, but also in complexity theory this line of attack dates back to Berman and Hartmanis, where the structural property examined was sparseness, and many results are well-known.

The structural properties we identified are, among others: -robustness. A complete set is robust if it stays complete under the operation of set difference with sets of different sorts -mitoticity. A set is mitotic if it can be split into two sets that are in the same degree as the original set. -auto-reducibility. A set is auto reducible if membership question to the set can be solved by asking questions to the same set, excluding the input.

These properties have relations to each other, e.g., some forms of mitotic sets are auto-reducible and some sets that are not auto-reducible are also not robust for that reason. We proved results on these properties that do not relativize, a great obstacle in other lines of attack on the separation problem. Also, the "B does not have property P" part of the proof can be done for complexity classes high up in the time hierarchy that allow for diagalization against P, and then translate to classes of more central interest. E.g.,if complete sets of say EXP can be shown not to have a property P that EXPSPACE classes do have, then PSPACE is not EXP.

Moreover if for classes $A < B < C$ class A can be shown to have the property whereas C does not, then a proof or disproof of propterty P for B gives a separation either way.

On Sparse Self-reducible Sets

Falk Unger (CWI - Amsterdam)

Building up on the work of Lozano & Toran [1991] we prove new results about sparse self-reducible sets.

We define tree-self-reducibility and prove that sparse *tt*-self-reducible sets are in $\mathsf{P}^{\mathsf{NP}[\log]}$. This upper bound seems to be tight since we can exhibit a sparse *tt*-self-reducible set which is in but not lower than $\mathsf{P}^{\mathsf{NP}[\log]}$ in some relativized world.

We finally prove that log-sparse *btt*-self-reducible sets are in P.

Keywords: Computational Complexity, Self-reducible, Sparse, Low Density, Tree

Joint work of: Buhrman, Harry; Torenvliet, Leen; Unger, Falk