abstracts

- Monday, 27 September 1999
  Michael Saks, Rutgers University
  An Improved Exponential-time Algorithm for k CNF Satisfiability
  Abstract: In this talk, I'll present and analyze a simple randomized algorithm for the satisfiability problem for k-CNF formulas. For each k, the expected running time of our algorithm on any k-CNF formula is significantly better than 2^n, and the bounds for general k-CNF are the best known for worst-case input. In particular, on input a satisfiable 3-CNF formula, the algorithm finds a satisfying assignment in time 0(1,37^n) with high probability. The best previous algorithm for 3-CNF formulas had running time 0(1.49^n). (A recent new algorithm of Schoening does better than ours for 3-CNF formulas, but not as well for K-CNF formulas).
  If time permits, I'll also discuss an application of our methods to circuit complexity lower bounds.
  This is joint work with Mohan Paturi, Pavel Pudlak and Francis Zane.

- Monday, 4 October 1999
  Leonid Gurvits, NECI
  Operator Scaling and Approximating the Mixed Discriminant
  Abstract:

- Monday, 11 October 1999
  Ran Raz, The Weizmann Institute of Science, Israel
  Exponential Separation of Quantum and Classical Communication Complexity, and some Geometrical Properties of the Sphere S^n
  Abstract:

- Monday, 18 October 1999
  There is no talk scheduled for this date

- Monday, 25 October 1999
  Eldar Fischer, Tel Aviv University
  Graph Embeddings via the Regularity Lemma
  Abstract: A graph embedding result is the formulation of conditions for a graph G, that ensure it contains a subgraph H with specified properties. The Regularity Lemma of Szemeredi ensures the existence of an approximation of G (by a small structure), so

that most of the specific details of G conform roughly to the "typical case" with respect to the approximation.
This lemma allows the proving of graph embedding results by applying (somewhat simpler) results to the approximation of G. Results about the existence of many distinct copies of H ("abundance") in some instances where H is a fixed graph can also be proven.
Some applications of the Regularity Lemma are presented. Among them are a generalization of the result of Alon and Yuster regarding the minimum degree of G ensuring the existence of (1-o(1))|G|/|K| vertex disjoint copies of a fixed graph K, and results about the existence of specified 2-factors in G. A new method for using the Regularity Lemma in the context of induced subgraphs is also presented; it is used for proving results which are relevant to the testability of graph properties.

- Monday, 1 November 1999
  There is no talk scheduled for this date

- Monday, 8 November 1999
  Eli Ben-Sasson, Hebrew University
  Many Hard Examples for the Polynomial Calculus
  Joint work with Russell Impagliazzo, from UCSD
  Abstract: A CNF formula (an AND of ORs) can be naturally encoded as a set of boolean valued polynomials, where "boolean valued" means restricting all variables to {0,1} assignments (this can be done by adding the polynomial x(1-x) for each variable x).
  A CNF formula is unsatisfiable <=> the set of defining polynomials has no common root <=> the polynomial 1 is in the ideal generated by these polynomials (Hilbert's Nullstelensatz).
  Main Question
  What is the minimal degree of the unsatisfiability proof of a set of boolean polynomials ? where a proof is a demonstration that 1 is in the ideal.
  Main Answer
  For a randomly chosen 3-CNF, with n variables and cn clauses (for large enough constant c), with high probability the degree (=complexity) of the proof is linear, whenever the charactaristic of the field is > 2. This lower bound is optimal, because in the boolean case there always is a linear degree proof.
  This result can be naturally stated in the Algebraic context, with no reference to "proof-complexity".
  Talk Outline
  1) Proof Complexity and connections to Complexity. 2) Polynomial Calculus - motivation and definitions. 3) A complete simple proof of the main answer mentioned above, involving elementary combinatorics and elementary algebra.

  For those who have attended Prof. Razborov's lecture: this lecture will be a direct continuation, giving more details for a concrete example.
  Main Question
  What is the minimal degree of the unsatisfiability proof of a set of boolean polynomials ? where a proof is a demonstration that 1 is in the ideal.

Main Answer For a randomly chosen 3-CNF, with n variables and cn clauses (for large enough constant c), with high probability the degree (=complexity) of the proof is linear, whenever the charactaristic of the field is > 2. This lower bound is optimal, because in the boolean case there always is a linear degree proof.
This result can be naturally stated in the Algebraic context, with no reference to "proof-complexity".
Talk Outline
1) Proof Complexity and connections to Complexity. 2) Polynomial Calculus - motivation and definitions. 3) A complete simple proof of the main answer mentioned above, involving elementary combinatorics and elementary algebra.

For those who have attended Prof. Razborov's lecture: this lecture will be a direct continuation, giving more details for a concrete example.

For those who didn't: the talk will be completely self-contained.

- Monday, 15 November 1999
  Jeff Kahn, Rutgers University
  Entropy, Independent Sets and Antichains
  Abstract: "Dedekind's Problem" of 1897 asks for the number, say f(n), of antichains in the Boolean algebra of subsets of [n].
  In 1969 Kleitman showed that log(f(n)) is asymptotic to the middle binomial coefficient (call it b(n)), and a 1975 improvement by Kleitman and Markowsky showed that the error term is not more than O(logn/n)b(n). Then Korshunov (1981) and later Sapozhenko (1989) determined the asymptotics of f(n) itself.
  Proofs of the preceding results range from difficult to impenetrable. Our main goal in this talk will be to sketch an entropy-based "book" proof of the Kleitman-Markowsky bound. What we actually prove is an exact bound for general graded partial orders, which, somewhat curiously, specializes to essentially K-M in the case of a Boolean algebra.
  Time permitting, we will also say a little about the proof of a conjecture of Benjamini, Haggstrom and Mossel on the expected range of "cube-indexed random walk."

- Monday, 22 November 1999
  Luca Trevisan, Columbia University
  A PCP Characterization of NP with Optimal Amortized Query Complexity
  Abstract: For any epsilon>0 and any sufficiently large integer q, we present a characterization of NP in terms of a Probabilistically Checkable Proof (PCP) system where the verifier makes q queries and has error probability at most 2^{-(1-epsilon)q}. The trade-off between number of queries and error probability is essentially optimal. Such a characterization gives improved (and essentially tight) non-approximability results for Boolean constraint satisfaction problems, separation

results between the power of different PCP models, and a new (simpler) proof of Hastad's non-approximability result for the Maximum Clique problem.
Our result is obtained via the following steps:

1) The introduction of a general method to perform "dependent iterations" of a basic verifier.

2) The analysis of the iterated version of a 3-query "inner" verifier by Hastad.

3) The proof of a new "composition theorem" to convert the inner verifier obtained with the above steps into a PCP characterization of NP.

(Joint work with Alex Samorodnitsky and Madhu Sudan)

- Monday, 29 November 1999
  Leslie G. Valiant, Harvard University
  Robust Logic
  Abstract: It has been recognized for centuries that cognitive phenomena exhibit both inductive as well as deductive aspects. The processes of induction and deduction have been studied systematically though separately in the frameworks of computational learning and computational logic. Since cognitive computations appear to perform these processes in combination, a single framework is required within which the two can be discussed simultaneously. Robust logics are designed to serve just that purpose. They are based on the view that a knowledge-base can be made robust only if each assertion in it is verifiable empirically against and learnable from real world observations. The challenge then is to reconcile this with the advantages offered by conventional logics, in particular a sound basis for deduction. Robust logics are designed to bridge this gap while retaining computational feasibility. In this framework both the computational work as well as the accuracy of both learning and deduction are polynomially controlled.

- Monday, 6 December 1999
  Ehud Friedgut, MSRI and UC Berkeley
  Projections of Subsets of the Discrete and Continuous Cube
  Abstract: *Easy question: Can you find a subset of [0,1]^n of volume 1/2 such that every n-1 dimensional projection is of volume 1/2 + O(1/n)?
  *Hard: Can you find such a subset of the discrete cube {0,1}^n?

  *Harder: Can you find a subset of [0,1]^n for which the above is true both for the set and its complement?

  All the above are questions about a notion that arises naturally in game theory, percolation theory and other settings, the notion of the influence of a variable on a Boolean function on a product space.

We will review some of the known results and concentrate on showing how the continuous case can be easily deduced from the discrete case.

- Monday, 13 December 1999
  Dorit Aharonov, UC Berkeley
  A Quantum to Classical Phase Transition in Noisy Quantum Computers
  Abstract: The fundamental problem of the transition from quantum to classical physics is usually explained by decoherence, and viewed as a gradual process. The study of entanglement, or quantum correlations, in noisy quantum computers implies that in some cases the transition from quantum to classical is actually a phase transition.
  I will present recent results in which it is shown that the "entanglement length" (to be defined in the talk) in noisy quantum computers exhibits a phase transition at a critical noise rate, where it transforms from infinite to finite. Above the critical noise rate, macroscopic classical behavior is expected, whereas below the critical noise rate, subsystems which are macroscopically distant one from another can be entangled. The macroscopic classical behavior in the super-critical phase is shown to hold not only for quantum computers but also for more general quantum systems. This phenomenon provides a possible explanation to the emergence of classical behavior in these systems.

  I will present many open problems in various fields which are raised by this result: questions related to statistical quantum physics (eg. find critical exponents, provide renormalization group analysis, connection to other quantum phase transitions), to the foundations of quantum mechanics, to the theory of quantum error correction, to cellular automata, and more. The proof uses a map to classical percolation, and the threshold result for fault tolerant quantum computation. No prior knowledge will be assumed, except for some basic idea of what quantum computation means.

  (The paper can be downloaded from this URL address:
  http://arXiv.org/find/quant-ph/1/au:+aharonov/0/1/0/past/0/1)

- Monday, 17 January 2000
  Jozsef Beck, Rutgers University
  The Erdos-Szekeres Game
  Abstract:

- Monday, 24 January 2000
  Alex Samorodnitsky, IAS
  On the optimum of Delsarte's linear program
  Abstract: We are interested in the maximal size A(n,d) of a binary error correcting code of length n and distance d, or, alternatively, in the best packing of balls of radius (d-1)/2 in the n-dimensional Hamming space. The best known lower bound on

A(n,d) is due to Gilbert and Varshamov, and is obtained by a covering argument. The best known upper bound is due to McEliece, Rodemich, Rumsey and Welch, and is obtained using Delsarte's linear programming approach. It is not known, whether this is the best possible bound one can obtain from Delsarte's linear program. We show that the optimal upper bound obtainable from Delsarte's linear program will strictly exceed the Gilbert-Varshamov lower bound. In fact, it will be at least as big as the average of the Gilbert-Varshamov bound and the McEliece, Rodemich, Rumsey and Welch upper bound. Similar results hold for constant weight binary codes.

- Monday, 31 January 2000
  Yuval Peres, Hebrew University
  Two Erdos problems on lacunary sequences: Chromatic number and diophantine approximation
  Abstract: Let {n_k} be an increasing lacunary sequence, i.e., the ratio between successive elements is at least 1+1/M for some M. Erdos considered a graph G on the integers, where two integers are connected if their difference is in the sequence {n_k}, and asked for the chromatic number Chi(G). Y. Katznelson found a connection to a Diophantine approximation problem (also due to Erdos) and bounded Chi(G) by M^2 (with a logarithmic correction). We apply the Lovasz local lemma to this Diophantine problem, and prove that Chi(G)< CM\log(M). This is sharp up to the \log factor. Joint work with Wilhelm Schlag

- Monday, 7 February 2000
  Noga Alon, Tel Aviv University
  Economical covers with geometric applications
  Abstract: What is the typical minimum number of lines needed to separate n random points in the unit square? The study of this question leads to related problems for finite projective planes and to certain extensions of the known results about the existence of economical covers in simple uniform hypergraphs.
  Joint work with B. Bollobas, J. H. Kim and V. Vu.

- Monday, 14 February 2000
  Madhu Sudan, MIT
  List decoding of error-correcting codes
  Abstract: Error-correcting codes are combinatorial objects designed to deal with the problem of noise in information transmission. A code describes how to judiciously add redundancy information that recovers from a small amount of (even malicious) corruption. ``Recovery'' here is interpreted as follows: If a small number, say d, of errors occur, then it is possible to detect that errors have occurred. For an even smaller number, classically d/2, one can even find which locations are in error and fix them. Among the simplest and yet very efficient error-correcting codes are codes based on properties of low-degree polynomials, called Reed Solomon codes. In this talk we will describe a simple algorithm for recovering from error in Reed Solomon codes. One of

the novel features of this algorithm is that it recovers from much more than the above-mentioned bound of d/2 that classical algorithms could tolerate.
Joint work with Venkatesan Guruswami (MIT).

- Tuesday, 15 February 2000
  Johan Hastad, Royal Institute of Technology
  Some optimal inapproximability results
  Abstract: Using very efficient probabilistically checkable proofs (PCP) for NP we prove that unless NP=P, some of simple approximation algorithms for basic NP-hard optimization problems are essentially optimal. In particular given a SAT formula with exactly 3 variables in each clause it is not hard to find an assignment that satisfies a fraction 7/8 of the clauses. We prove that (upto an arbitrary $\epsilon >0$) this is the best possible for a polynomial time approximation algorithm.
  In this talk we concentrate on the problem of given a linear system of equations mod 2, to satisfy the maximal number of equations. This problem is easy to approximate within a factor of 2 and we prove that this is essentially tight. This result is obtained by constructing a PCP that uses logarithmic randomness, reads 3 bits in the proof and accepts based on the exclusive-or of the these bits. This proof system has completeness $1-\epsilon$ and soundness $1/2+\epsilon$.
  This result improves the non-approximability constants for a number of problems, in particular for MAX-CUT, MAX-2-SAT, MAX-DI-CUT and VERTEX COVER.

- Monday, 28 February 2000
  Ronen Shaltiel, IAS
  Extracting Randomness via Repeated Condensing
  Abstract: Extractors are functions that allow, in some precise sense, extraction of randomness from somewhat random distributions, using only a small number of additional truly random bits. A lot of effort has been devoted to constructing explicit (polynomial time computable) extractors which use a short seed and extract as much as possible random bits. Still, explicit constructions do not achieve the parameters of the "optimal extractor", (whose existence is proven using the probabilistic method, and matches the known lower bounds).
  In this talk we show how to construct efficient condensers, where a condenser is a function which given a random soucre, (and a short seed) constructs a new source of smaller length which contains (roughly) the same amount of randomness as the initial source. Extractors are then constructed by repeatedly condensing the initial source.

  We use these ideas to construct the following explicit extractors:

  - An extractor that uses a seed of the optimal length ($O(\log n)$) and extracts $1 / \log n$ of the initial randomess in the source. - An extractor that uses a seed of length $O(\log n \log \log n)$ and extracts any constant fraction of the initial randomness in the source.

  (n denotes the length of strings in the source).

This is joint work with Omer Reingold and Avi Wigderson

- Monday, 06 March 2000
  Peter Winkler, Bell Labs
  Percolation and Collision
  Abstract: Two tokens take simple random walks on the same graph G. The "clairvoyant demon" conjecture says that if the walks are known, then (with positive probability) they can be scheduled so that they never collide. This conjecture remains open.
  We show that if the tokens can be moved backward as well as forward, then they can indeed be advanced arbitrarily far without colliding. The result can be restated in terms of dependent percolation on the plane grid. For example, if the axis nodes are labelled by random numbers from 1 to 4 and nodes are destroyed when their X- and Y-labels coincide, then an infinite component remains. (Similar results have been obtained independently by Ballister, Bollobas and Stacey, using a different approach.)

  The original problem translates to ORIENTED percolation and remains notoriously open, even when 4 is replaced by a million. We will give some indication of what has prevented us (and perhaps others) from proving the conjecture. Finally, we will present a new percolation problem of a similar type.

- Monday, 13 March 2000
  Benny Sudakov, IAS/Princeton University
  Max Cut and the Smallest Eigenvalue
  Abstract: If G=(V,E) is an undirected graph, and S is a nonempty proper subset of V, then (S,V-S) denotes the cut consisting of all edges with one end in S and another one in V-S. The MAX CUT problem is the problem of finding a cut of maximum size in G. This is a well known NP-hard problem and the best known approximation algorithm for it, due to Goemans and Williamson, is based on semidefinite programming and an appropriate (randomized) rounding technique. It is proved that the approximation guarantee of this algorithm is roughly 0.878. By constructing appropriate graphs, Karloff showed that this minimum can be attained for the graphs whose Max Cut has exactly 0.844|E(G)| edges.

  Goemans and Williamson also proved that their algorithm has a better approximation guarantee for graphs with larger cuts. Here we show that this analysis is also tight. Our construction is based on the properties of graphs arising from the Hamming Association Scheme and extends and simplifies the result of Karloff. We also show how it can be use to analyze some other best known approximation algorithms related to Max Cut.

  (This is joint work with N. Alon and U. Zwick)

- Monday, 27 March 2000
  Andrew Yao, Princeton University
  On Quantum Complexity of Graph Properties
  Abstract: For any boolean function f of n variables, let D(f) be the minimum number of variables needed to be examined by any decision tree computing f, and let Q(f) be its quantum analogue with an epsilon error permitted. It has been conjectured that the quantum speed up obtainable is at most quadratic, ie, Q(f) \geq D(f)^1/2, which in particular would imply Q(f) \geq n for any nontrivial monotone n-vertex graph property f. In this talk we take a step towards resolving this latter conjecture by proving Q(f) \geq n^2/3 for all such f. We also discuss the quantum complexity of specific graph properties; for example, we show that Q(f) = n^{3/2} where f(G) = 1 if and only if G has an even number of connected components.

- Monday, 03 April 2000
  Russell Impagliazzo, UC San Diego
  Convex complexity measures
  Abstract: We don't know whether NP-complete problems have exponential complexities, polynomial complexities or something in-between. In fact, it is conceivable that the complexity varies as the input size changes, alternating between polynomial and exponential complexity. Thus, whether for practical purposes $P=NP$ holds might in some sense be dependent on the technology level.
  In this talk, we re-examine whether this a priori possibility is indeed possible. In particular, we change the measure of instance complexity from size to two parameters, dimension (number of independent choices that need to be made) and granularity (number of options for each choice). Then we show that the exponent of worst-case complexity is decreasing with the dimension. As a consequence, if the complexity is sub-exponential for infinitely many values of dimension, then it is asymptotically sub-exponential. We show this behaviour for constraint satisfaction, independent set, and some version of satisfiability.

  This is joint work with Avi Wigderson and Mohan Paturi.

- Monday, 17 April 2000
  Alexander Razborov, IAS/Princeton University
  Pseudorandom Generators in Propositional Proof Complexity
  Abstract:

- Monday, 24 April 2000
  Bela Bollobas, Memphis and Cambridge
  Polynomial Invariants of Graphs On Surfaces
  Abstract:

- Monday, 01 May 2000
  Gregory Freiman, Tel Aviv University
  Analytical Methods in Integer Programming
  Abstract: The present reseach is dedicated to the development of a structural approach to Integer Programming and is based on the application of analytical methods of Additive Number Theory. Important case of "dense" problems is discussed when the size of domain of a function is greater than the range of this function. Algorithms were designed which are in many cases linear O(m), m being the number of unknowns.

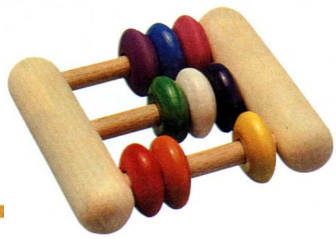
- Monday, 08 May 2000
  Omer Reingold, AT&T and IAS
  Selective Decommitment, Magic Functions and 3-Round Zero-Knowledge
  Abstract: The foundation of cryptography has provided powerful primitives and protocols. Unfortunately, in some cases, their behavior under composition is still poorly understood. This may lead to very undesirable consequences. Consider for example a merchant putting the encryptions of one hundred songs on a CD. This CD is provided for free and the decryption key of each individual song can be purchased over the Internet. It turns out that our current knowledge cannot even rule out the unfortunate situation where a customer can select fifty encryptions to be opened (songs to be purchased) and extract (steal) a fifty-first song.
  In this talk we discuss this problem of "selective decryption" (in the related form of "selective decommitment"). We manage to relate this problem to two additional fundamental problems: the existence of what we term "magic functions" and the existence of three-round zero-knowledge arguments for non-trivial languages. We also give some positive results for selective decommitment (though this important problem is far from being solved by our work).

  A surprising result of our work is the connection between selective decommitment and the existence of magic functions. Consider the well known and intuitively appealing Fiat-Shamir methodology for converting (easy to design) identification schemes into (harder to design) digital signature schemes. This approach requires what we term "magic functions". We show that if selective decryption behaves as one expects (the fifty-first song is still secure), then there are no magic functions (it is not a perfect world).

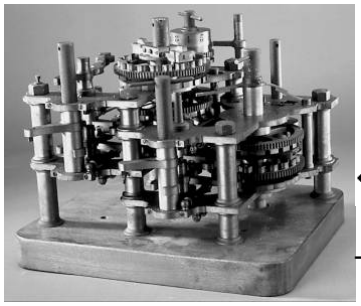
  Joint work with Cynthia Dwork, Moni Naor and Larry Stockmeyer

Sponsored by:

[National Science Foundation](#)

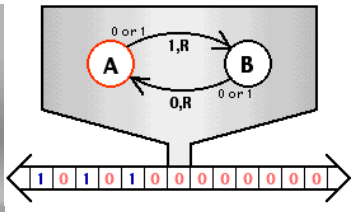


Abacus

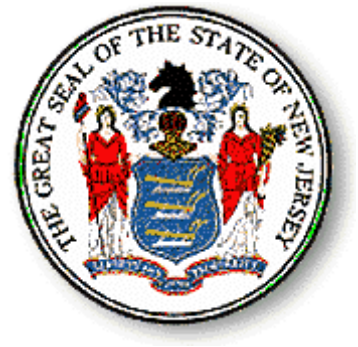


"Analytical Engine"

by Charles Babbage



Turing Machine



[State of New Jersey](#)