DIMACS Special Year on Computational Intractability

The DIMACS Special Year on Computational Intractability commenced in September 1999, when DIMACS was in the final months of its NSF "science and technology center" grant, and ended on August 31, 2001.

The notion of computational intractability lies at the heart of computer science, and is central to the interface between discrete mathematics and theoretical computer science. Research on intractability has two long range goals:

- 1. To identify which computational problems are tractable and which are intractable.
- 2. To develop algorithmic strategies for dealing with problems which are intractable.

These two aims have been the subject of intense research efforts over the past twenty five years, and these efforts have been extremely fruitful with a wealth of fundamental results, both positive and negative results in areas such as approximation algorithms, circuit lower bounds, and the relationship between intractability and randomized computation.

The DIMACS Special Year on Computational Intractability was aimed at refocusing of efforts, in order (i) to consolidate and build on the substantial body of knowledge and techniques that have been developed in the past, and (ii) to identify the next set of research directions and subgoals that will move us towards the ultimate goals of the field.

To this end, we brought together a large number of people in the special year, in the usual DIMACS mode of bringing together people with different backgrounds and points of view. The activities of the special year included workshops focused on the role of pseudorandomness in complexity theory, probabilistic analysis of algorithms for hard problems, approximation algorithms for NP-hard problems, exact algorithms for NP-hard problems, cryptography and intractability, and intrinsic complexity of computational problems. In each case, the workshops served the main goals of bringing together a variety of people to review progress in the subarea covered by the workshop, and to discuss new directions and research problems.

The interactions between researchers, in the workshops, through the visitor program and our seminar series, led to new directions of research and new research challenges for the future, as hoped, as well as a large number of exciting new results. The subject was, as hoped, given a renewed sense of energy. Specific research contributions are surveyed in another section of this report.

Organizing Committee

Michael Saks (Chair), Rutgers University
David Johnson, AT&T Labs
Christos Papadimitriou, University of California-Berkeley
Eva Tardos, Cornell University
Avi Wigderson, Hebrew University and Institute for Advanced Study
Andrew Yao, Princeton University

1 Workshops

- **Pseudorandomness and Explicit Combinatorial Constructions**
  Dates: October 12 - 15, 1999
  Location: CoRE Building, Rutgers University
  Attendance: 94
  Organizers: David Zuckerman, University of Texas and UC Berkeley; Russell Impagliazzo, University of California at San Diego; Amnon Ta-Shma, International Computer Sciences Institute

  The two topics appearing in the title of this workshop represent important and closely linked research directions within, respectively, computer science and combinatorics.

  The question of the power of randomness in computation is a central theme within the theory of intractability. The central question is: "are there problems that are intractable using deterministic computation that are tractable using randomized computation?" Research on this question, which points to a negative answer, has focused around the study of the constructibility of pseudo-random generators, and the constuctibility of these generators has been shown to be closely connected to the existence of computational problems that are suitably intractable. The development of the probabilistic method in combinatorics has led to a variety of non-constructive proofs of existence of combinatorial objects satisfying certain specified properties: graphs whose clique and independence numbers are both very small (Ramsey graphs), graphs with strong connectivity properties, such as expanders, and large codes with optimal distances. It has long been of interest to find explicit constructions of objects with these properties.

These two areas are brought together by the realization that the problem of designing pseudorandom generators, and related problems such as that of making randomized algorithms robust in the presence of imperfections in the random source, can be formulated as problems of explicit construction of combinatorial objects. Thus the study of such constructions has become an important part of the theory of probabilistic computation The problem of proving lower bounds on computational problems (at least in non-uniform models) can be viewed as that of finding an explicit hard function, where it is known non-constructively that most functions are hard.

The computational point of view has motivated new problems in combinatorics and also led to new techniques for constructing objects like expanders that are better than any known before. This symbiosis is also evident in the connection between the theory of derandomization in computational geometry and discrepancy theory within combinatorial geometry.

This workshop focused on this common area of interest, focusing on problems and techniques for construction of combinatorial objects arising in computer science, graph theory, and coding theory. In recent years, these techniques have included methods from such diverse areas as representation theory and algebraic geometry, and one aim of the workshop was to expose a broader range of researchers to these techniques.

The plenary talks were given by:

Noga Alon, Tel Aviv University. Topic: Ramsey Type Graphs.

Amin Shokrollahi, Bell Labs. Topic: Codes Over Algebraic Curves.

Luca Trevisan, Columbia University. Topic: Extractors and Pseudorandom Generators.

Avi Widgerson, IAS and Hebrew University. Topic: Open Problems.

- **Probabilistic Analysis of Algorithms for Hard Problems**
  Dates: November 1- 3, 1999
  Location: Fiber Optic Materials Research Building, Rutgers
  University Attendance: 78
  Organizers: Alan Frieze, Carnegie Mellon University; Martin Dyer, University of Leed

  The analysis of algorithms for NP-hard problems under distributional assumptions on the input, is an important approach to dealing with hardness issues. As Karp remarked in his Turing award lecture, "I felt, however, that in the case of NP-complete problems we weren't going to get the worst-case guarantees we wanted, and that the probabilistic approach was the best way and perhaps the only way to understand why heuristic combinatorial algorithms work so well in practice." Random models are also important as benchmarks for empirical testing of algorithms.

  Here tools from probability theory (especially concentration inequalities), and the theory of random combinatorial structures, especially random graphs, play an important role. Problems such as finding Hamilton cycles in graphs or properly coloring them have been shown to be tractable under such assumptions. Simple heuristics have been defined which are likely to be asymptotically close to optimal with high probability. The paper of Karp on the TSP in the plane was of this type and was fundamental in stimulating interest in the subject. There are also, hybrid approaches, such as the analysis of semi-random models which combine aspects of worst case and average case analysis.

  Sometimes there are results which show that the average case can be hard too. Many enumerative type algorithms have been shown to take exponential time with high probability. Of particular importance here is the result of Chvatal and Szemeredi showing that a certain random model of satisfiability, resolution can take exponential time with high probability. Levin introduced the notion of completeness on average to describe probabilistic models problems which are unlikey to have fast average case solution.

There are a variety of research goals: to extend average case analysis to new problems, to explore the effect of distributional assumptions on the behavior of algorithms, to identify distributions that are especially hard for particular problems.

The workshop brought together researchers interested in all of these approaches. Dick Karp spoke about "Matchings, Cores and Dense Subgraphs in Sparse Random Graphs," Van Vu on "Approximation of the Independence Number," and Tomas Luczak on "Random Graphs and Positional Games." Also, C.R. Subramanian presented a talk on "A BFS Approach to Partitioning Problems on Random Graphs," A. Czumaj one entitled "Towards an Algorithmic Version of the General Lovasz Local Lemma," David Matula one on " A Cell Occupancy Sieve Algorithm Resolving Hardest Case Roundings of Floating Point Functions," and R. Venkatesan one on "Random Cayley Graphs and Discrete Log." Other featured talks included "The Tale of One-Way Functions" by L.Levin, "Information Storage in Finite Memory" by S. Venkatesh, "Case Studies in Torpid Mixing" by Mark Jerrum, "An Extension of Path Coupling" by L. Goldberg, "Expected Length of Longest Common Subsequences" by Gene Lueker, and " Fast Randomized Algorithms for Stochastic Programming Problems" by L. Stougie. Greg Sorkin talked about "A Biased Walk Through Simulated Annealing," M. Furer about "Approximating Permanents of Complex Matrices," Joel Spencer about "Random Sequential Greedy," S. Vempala on "Inapproximability via the Probabilistic Method," and J. Yukich on "A survey of the probability theory of the Euclidean TSP." Christian Borgs presented "Slow Mixing on the Hypercubic Lattice," D. Achlioptas presented "Mick gets more than pie," John Franco "A Perspective on Certain Polynomial Time Solvable Classes of Satisfiability," J. Kim "Random 2SAT," Peter Winkler " Optimality and Greed in Dynamic Allocation," Angelika Steger "Balanced Allocations: More Balls than Bins," A. Rucinski " Embedding Sparse Graphs into Dense Regular Graphs," Ed Coffman "Interval Packing in One and Two Dimensions," and finally David Johnson presented "Average-Case Analysis of a Self-Organizing Bin Packing Algorithm."

- **Computing Approximate Solutions to NP-Hard Problems**
  Dates: February 20 - 22, 2000
  Location: Princeton University
  Attendance: 63
  Organizers: Sanjeev Arora, Princeton University; Eva Tardos, Cornell University; Luca Trevisan, Columbia University

  This workshop focused on the design and analysis of approximation algorithms, heuristics that compute solutions whose value is provably within some fixed factor of the optimal. Although interest in approximation algorithms intensified in the 1970s soon after the discovery of NP-completeness, the area has truly blossomed only in the past decade. Amazing progress has ocurred both in our ability to design approximation algorithms, and in proving limits to approximability. Approximation algorithms have been designed for many important problems such as balanced cut, network design, Euclidean TSP, facility location, and a number of scheduling problems. In the process, many simple and broadly-applicable techniques have emerged, such as rounding followed by dynamic programming, and more recently, the rounding of solutions obtained from linear or semi-definite relaxations, primal-dual methods, geometric embeddings, and the geometric divide-and-conquer approaches used for Euclidean TSP.

  Also in the past decade, in an effort to prove limits on approximability, the notion of probabilistically checkable proof was invented in complexity theory to show that for some important problems such as clique, graph coloring and set cover, achieving a certain approximation ratio is no easier than solving the problem exactly.

  The workshop started with a set of plenary talks –geared to a broad audience– surveying the current state of the art in this growing area. They were followed by talks on recent results in approximation algorithms and lower bounds.

The field of approximation algorithms has many open questions. A resolution of these questions would require new ideas in either algorithm design or in proving inapproximability. By simultaneously focussing on these complementary areas of research, we hope to foster further interactions between researchers working in them. The goal is to arrive at a better understanding of the limits of the known techniques in both areas and to focus attention on the main open problems.

The workshop also examined practical aspects of approximation algorithms. We strongly believe that the same ideas that lead to provable worst case guarantees can give better quality solutions in practice than known heuristics. Indeed, existing implementations of approximation algorithms in most cases provide solution a lot closer to optimum than guaranteed by the worst case bound. Even better, in many cases the algorithm also provides very good lowerbounds on the optimum, thus allowing it to prove that the solution found for the particular problem instance is quite close to optimum. These and other issues related to performance and implementation were explored at the workshop.

- **Mini-Workshop: Faster Exact Solutions for NP Hard Problems**
  Dates: February 23 - 24, 2000
  Location: Princeton University (Nassau Inn), Princeton, NJ
  Attendance: 49
  Organizers: Mohan Paturi, University of California at San Diego; Richard Beigel, University of Illinois - Chicago

  We seek out faster exact solutions for NP-hard problems not only for their own sake, but also in order to gain insights into complexity. This workshop was organized to specifically examine the following topics for NP-hard problems:

  1. Algorithms with improved exponential-time complexity
  2. Relationships among the complexities
  3. Obstacles to subexponential algorithms
  4. Heuristics for faster exponential-time algorithms and empirical studies

  The workshop consisted of 12 half-hour contributed talks and a one hour invited talk presented by Bart Selman (Cornell University).

  The opening talk was by Philip Klein (Brown University) who spoke on “Finding the closest lattice vector when it’s unusually close” followed by a presentation by David Eppstein (University of California, Irvine) presentation on “An Exact Algorithm for 3-Coloring.” Mike Robson (Universite de Bordeaux) spoke on “Maximum Independent Set Algorithms: Improved Analysis,” followed by Vadim Lozin (Rutgers University) on “Robust Algorithms for the Stable Set Problem .” The morning session ended with a talk by Richard Beigel (University of Illinois) on “Applying structions to the independent set problem.”

  The afternoon session began with “Algorithms for k-SAT based on Covering Codes” by Edward Hirsch (Steklov Institute of Mathematics at St. Petersburg) followed by Jens Gramm (University of Tuebingen) on “Faster Exact Solutions for Max2SAT.” Oliver Kullman, (University of Toronto) then spoke on “Using poly-time SAT decidable and recognisable hierarchies of conjunctive normal forms for improved SAT decision and general lower bounds on resolution with oracles.” Jianer Chen (Texas A&M University) spoke on “Improved Exponential Time Algorithms for Vertex Cover” and the day ended with a talk by Rolf Niedermeier (University of Tuebingen) “On Efficient Fixed Parameter Algorithms for Weighted Vertex Cover.”

  The second day of the workshop opened with an invited talk on “Satisfiability Testing: Theory and Practice” presented by Bart Selman (Cornell University) who was followed by a talk on “Exponential Algorithms for SAT and MAJSAT” by Michael Littman (AT&T Labs Research and Duke University). The workshop concluded with a talk on “Complexity of k-SAT” by Ramamohan Paturi (University of California, San Diego).

- **Cryptography and Intractability**
  Dates: March 20 - 22, 2000

Location: CoRE Building, Rutgers University
Attendance: 79
Organizers: Moni Naor, Weizmann Institute of Science; Joe Kilian, NEC Research Institute; Shafi Goldwasser, MIT and Weizmann Institute of Science

Cryptography is arguably the ultimate application of computational hardness. Almost every cryptographic task requires the existence of a one-way function, and some tasks seem to require even stronger hardness assumptions. Conversely, ideas from cryptography have been used to establish the intractability of computational tasks. The goal of the workshop was to explore this tight relationship.

The interplay between cryptography and complexity theory revolves around a number of basic themes. Among those explored in this workshop were:

- The minimal intractability assumptions required for various cryptographic tasks.
- The feasibility of basing cryptography on worst-case assumptions.
- The proper form for an intractability assumption.

The workshop also explored the relationship between cryptography and more specific areas such as computational learning theory, proof complexity, game theory and combinatorial optimization.

The workshop was designed to reach a broad audience via general plenary talks, but also included several more specialized talks appealing to researchers already working in the field.

The morning of the first day began with Ran Canetti speaking on "Resettable Zero-Knowledge", one of the latest frameworks for applying the theory of interactive proof systems to more complicated real-world settings. Then, Dan Simon discussed "The Cryptographic Uses of Oracle Separations." The morning talks concluded with Yuval Ishai, speaking on "Compressing Cryptographic Resources."

On the afternoon of the first day, Moni Naor spoke on "Why we need a complexity theory of moderately-hard functions," discussing the uses of functions that are difficult but not impossibly (exponentially hard) to compute. Cynthia Dwork spoke on, "Zaps and Apps," giving new techniques for decreasing the message complexity of a number of cryptographic protocols.

The second day was started off by Jacques Stern, giving a plenary talk on "Twenty Years of Lattice Reduction in Cryptology." The rest of the day was devoted to connections between multi-party games and cryptography. Rebecca Wright spoke on "Secure Multi-party Computation of Approximation," followed by Joan Feigenbaum, who spoke on "Sharing the Cost of Multicast Transmissions." In the afternoon, Yevgeniy Dodis continued this theme, illustrating connections between multi-party cryptographic games and more classical game theory in his talk, "A Cryptographic Solution to a Game Theoretic Problem." Tal Malkin then spoke on "The All-or-Nothing Nature of Two-Party Secure Computation," showing some general results on the power of two-party cryptographic games. Joe Kilian then continued this line of discussion, showing further connections with classical game theory, with "More General Completeness Theorems for Secure Two-Party Computation".

Michael Kearns began the third and last day with a plenary talk, "Computational Learning Theory and Cryptography: A Survey," discussing a number of surprising connections between cryptography and learning theory. Then, Omer Reingold discussed the unification of a number of seemingly disparate open problems in cryptography, with his talk, "Magic Functions". In the afternoon, Rafail Ostrovsky spoke on, "Recent Results on Single Database Private Information Retrieval." Finally, Steven Rudich concluded the conference with a talk on "Things You Can't Do With A Random Function".

We note that the technical papers presented at this workshop have been very well received by the theory of computation community. Within the theory of computation community, the two most influential conferences are the ACM Symposium on Theory of Computing and the IEEE Symposium of Foundations of Computer Science. By a quick count, at least seven of the talks presented at the workshop were also presented at one of these two conferences. Workshop attendees were treated to leading papers in the area, in some cases a half-year before their presentation in more formal conferences.

- **Intrinsic Complexity of Computation**
  Dates: April 10 - 13, 2000

Location: CoRE Building, Rutgers University
Attendance: 74
Organizers: Paul Beame, University of Washington; Steven Rudich, Carnegie Mellon University; Andrew Yao, Princeton University

Computational Complexity Theory is the study of how much of a given resource (such as time, space, parallelism, randomness, algebraic operations, communication, quantum steps, or proof length) is required to perform the computations that interest us the most. Four decades of fruitful research have produced a rich and subtle theory of the relationship between different resource measures and problems. At the core of the theory are some of the most alluring open problems in mathematics.

This workshop reviewed our progress in and prospects for proving lower bounds on the complexity of natural computational problems. To this end, we arranged for a distinguished list of plenary speakers to share their historical, philosophical, and technical perspectives:

Miki Ajtai, IBM Almaden **Lance Fortnow**, NEC, Princeton **Russell Impagliazzo**, UCSD, San Diego CA **Steven Rudich**, Carnegie-Mellon University **Avi Wigderson**, Institute For Advanced Study, Princeton and Hebrew University **Andrew Yao**, Princeton University

- **Sublinear Algorithms**
  Dates: September 24 - 27, 2000
  Location: Nassau Inn, Princeton, New Jersey
  Attendance: 89
  Organizers: Shafi Goldwasser, MIT; Prabhakar Raghavan, Verity; Ronitt Rubinfeld, NEC Research Institute; Martin Strauss, AT&T Labs - Research

  Recent advances in computing power and the trend toward interconnecting computers has resulted in a tremendous increase in the size of datasets that are gathered and considered useful. Such data sets come from a wide variety of sources; for example, they might contain information describing the structure or content of the world wide web, Internet traffic flow, traffic and clickstream patterns of individuals or large groups of users, warehoused operational data from enterprises, or ongoing measurements of scientific observations.

  The unprecedented scale of these data sets demands that we revisit traditonal notions of efficient algorithms. In many applications, this means that the computational resources used (computation time, storage space, or communication bits) be small relative to the size of the data. Because of the severity of the constraints, one might think that there is only hope for solving problems that can be solved by straightforward statistical sampling techniques.

  Surprisingly, researchers in several different areas of mathematics and computer science have recently shown that interesting results can be obtained under such sublinear constraints. Besides techniques from sampling, many of these results incorporate sophisticated algorithmic and combinatorial contributions to solve appropriate approximate variations of the problems. To study this emerging area, in our workshop, we brought together researchers working in several communities, including combinatorial and algebraic property testing, streaming algorithms, randomized algorithms, synopsis data structures, and communication complexity.

  The workshop focused on a few main topics; several talks were given in each of algebraic and combinatorial property testing and in streaming and sketching algorithms. Besides these, several talks were given that were deliberately chosen to be interdisciplinary, including talks on memory hierarchies and low-communication cryptography. The relationships between the techniques and questions of interest in each of the main topics and the interdisciplinary areas were not fully understood even by the organizers prior to the workshop. From the comments we received, however, it is our feeling that the attendees now share our view that it is natural to place these topics under a single umbrella. Thus it is our hope that this workshop will lead to future collaborations between researchers in these areas.

  We first describe the main topics and then the interdisciplinary talks.

  A property testing algorithm must distinguish between strings that have a certain property and strings that not only do not have the property, but are actually far from having the property, i.e., strings that need to be changed in a significant fraction of locations in order to be transformed into a string that has the property. For example, if the string is a list of numbers, a tester for the property of being in sorted order would distinguish lists which are sorted from those which need to be changed in a large fraction of the locations in order to make them sorted. Property testers for several algebraic and combinatorial properties have been constructed. The surprising fact is that for several of the properties studied, one can achieve running times which are sublinear in the size of the string. Furthermore, there are many properties for which the running times are constant.

A survey of property testers for combinatorial properties was given. Many of the property tests developed within this framework have led to approximation algorithms for various problems, including max cut and clustering. Several other talks were given on testers for combinatorial properties, including: testers for the property of being a monotone function; testers for geometric properties, such as convexity and clustering; testers for graph theoretic properties, such as the colorability number, transitivity of a tournament, expansion, lack of a forbidden subgraph or max cut size.

Property tests have been applied to functions, for example to test whether a function is close to some linear or low degree polynomial function. Such tests have in turn been used to construct probabilistically checkable proof systems and to design program checkers as defined by Blum and Kannan. A survey was given on these applications of property testers as well as the techniques used to construct them. Other talks were given which described testers for matrix properties, and testers which apply to floating point settings.

Other property testing talks included talks on testing the property that two distributions are similar and on faster testing with the assistance of an untrusted prover.

A streaming algorithm has limited memory and can make just a single pass over its input. There is a relationship between a low-communication protocol for computing a function and a streaming algorithm for the function. Roughly speaking, the limited memory contents of a streaming algorithm can serve as the limited communication between several parties in a protocol, and vice versa. The limited memory contents can also sometimes serve as a "sketch" or "synopsis data structure" for the original data. Several talks were presented on this subject, including talks giving algorithms for geometric and other distances between strings or permutations, for self-joins and other database operations, for clustering, and for tracking dynamic data structures. A talk describing recent work from traditional statistics presented related work that was probably new to most participants. Finally, a talk compared the power of making a small sample from a data set with making a single pass over the data with limited memory.

Modern computers often have a memory hierarchy–main memory is faster than cache memory, which is in turn faster than disk memory. An algorithm can feasibly process a gigabyte of data, provided that it takes full advantage of each disk block it retrieves–it it not feasible to make a linear number of disk accesses. Two talks were given on this subject.

Many cryptographic protocol constructions introduce communication overhead that is polynomial, but, in some cases, too expensive ever to be used. Several talks described cryptographic protocols that require only reasonable overhead and use only sublinear communication to solve a problem whose naive solution requires at least linear communication.

Finally, a survey talk on how to devise codes for which determining whether a string is close to a codeword can be done in sublinear time was given. Many of the techniques used in this talk are related to those used in algebraic property testing.

2 Educational Activities

The following special topics graduate courses were taught at Rutgers University:

- Quantum Computation, Spring 2001, Instructor Michael Saks
- Theory of Probabilistically Checkable Proofs, Spring 2001, Instructor Mario Szegedy

3 A Selection of Research Results

- **Time/space tradeoff lower bounds**

  The two most important resources needed to perform computations are computing time and memory. In many situations, there seems to be a trade-off between these two resources: the computation can be performed much more quickly if there is a lot of memory available. This raises the fundamental question: is this apparent tradeoff merely a reflection of our ignorance of algorithm design or is it an inherent fact about computation. This leads to the theoretical problem of identifying specific computational problems where restricting memory provably causes a substantial increase in computation time. These issues were presented and discussed both in the weekly Special Year in Computational Intractability (SYCI) seminar and in the SYCI Intrinsic Complexity of Computation workshop in April, 2000. These discussions and other interactions at DIMACS led to two new results in the area.

  There are two directions in which such results have been studied: in the uniform setting and the non-uniform setting. In the uniform setting, DIMACS postdoc Dieter van Melkebeek and DIMACS member Lance Fortnow obtained new results for time space tradeoffs for the satisfiability problem. In particular, they showed that satisfiability can not be solved in time $n^{1.618}$ by any random-access Turing machine using space $n^{o(1)}$, improving previous results of Fortnow and Lipton and Viglas.

  In the non-uniform setting, Paul Beame (SYCI workshop organizer and visitor), Michael Saks (DIMACS member and SYCI organizer), Xiaodong Sun (Rutgers graduate student), and Eric Vee (U.W. graduate student), proved time/space tradeoffs for various problems within the branching program model. This work built upon a previous breakthrough of Ajtai and improved it in three directions: (1) the tradeoff applies to 2-sided randomized algorithms, not just deterministic algorithms, (2) the quantitative results obtained were significantly stronger, and (3) the proofs are somewhat simplified.

  Further work by Beame and Vee grew out of questions raised at the Intrinsic Complexity of Computation workshop.

  P. Beame, M. Saks, X. Sun and E. Vee, Super-linear time-space tradeoff lower bounds for randomized computation, Proc. 41st IEEE Symp. on Foundations of Computer Science, 2000, 169-179. An expanded version is in preparation.

  P. Beame, Erik Vee, Time-Space tradeoffs, multiparty communication protocols and nearest neighbor problems, 2001, preprint.

  L. Fortnow and D. van Melkebeek, Time-space tradeoffs for nondeterministic computation, Proc. 15th IEEE Conf. on Computational Complexity, 2000, 2–13.

  D. van Melkebeek, Time-space lower bounds for satisfiability, Bulletin of the European Assoc. for Theor. Computer Science, 73 (2001) 57–77.

- **Computational depth**

  DIMACS postdoc Dieter van Melkebeek, DIMACS member Lance Fortnow and DIMACS graduate student visitor Luis Antones introduced and studied *computational depth* which is a measure of the amount of "nonrandom" or "useful" information in a string (in the spirit of Kolmogorov complexity). This led, among other things to the notion of a "shallow set" of strings, which is a generalization of sparse sets. They proved that any computable set reducible to a shallow set has polynomial size circuits. They also showed that if a boolean formula has a nonnegligible fraction of satisfying assignments of low depth then there is an efficient algorithm for finding a satisfying assignment.

  L. Antunes, L. Fortnow, D. van Melkebeek, Computational depth, in Proc. 16th IEEE Conf. on Computational Complexity, 2001, 266–273.

- **Approximation algorithms for min-sum k-clustering**

  As an outgrowth of their interactions at the SYCI workshop "Computing approximate solutions to NP-hard problems", Moses Charikar and Danny Raz wrote a paper (with Yair Bartal) giving the first polynomial time non-trivial approximation algorithm for the *min-sum k-clustering problem*. In this problem, the input is a finite metric space and an integer k, and the problem is to partition the points into k clusters so as to minimize the total sum of distances between pairs of points assigned to the same cluster.

- **Exact algorithms for Graph Bandwidth**

  Following the SYCI workshop "Faster exact solutions to NP-hard problems" and inspired by the subject of the workshop, workshop participant and DIMACS visitor Uri Feige worked with DIMACS member Joe Kilian to design an exact algorithm for the graph bandwidth problem that runs in simple exponential time (as compared to the $n!$ naive algorithm). They also showed that Bandwidth has no subexponential time algorithm unless 3SAT does. This work appeared in:

  > Uriel Feige, Coping with the NP-hardness of the graph bandwidth problem, in Proc. SWAT 2000, Magnus Haldorsson (Ed.), Lecture Notes in Computer Science 1851, Springer, pages. 10–19.

- **Diagonalization as a tool for proving complexity lower bounds**

  DIMACS member Lance Fortnow gave a plenary lecture at the SYCI workshop on Intrinsic Complexity of Computation, surveying the role of diagonalization in complexity theory and speculating on the ways that it might be used in the future to attack some of the major open problems in the field. This became the basis of a survey article:

  > L. Fortnow, Diagonalization. Bulletin of the European Association for Theoretical Computer Science, 71: 102-112, June 2000.

- **A simple graph theoretic construction of expanders**

  Expanders are graphs that are sparse, but nevertheless highly connected. Such graphs have been used to address many fundamental problems in computer science in a variety of areas, including complexity theory, derandomization, coding theory and cryptography. Standard probabilistic arguments show that almost every constant degree (≥ 3) graph is an expander. However, explicit constructions of expanders, which are important for many of the applications, are much harder and there has been an extensive body of research, mostly in mathematics, to accomplish this. The most famous construction, due to Lubotzky, Phillips and Sarnak, is a simple group theoretic construction, but the proof that it is an expander requires substantial and deep mathematics. It has remained a major challenge to give both a construction that is simple and has an elementary proof.

  The SYCI workshop on "Pseudorandomness and explicit combinatorial constructions" was focused around the role of explicit combinatorial constructions in complexity theory, and expanders were prominently featured in the workshop. At the workshop, Omer Reingold (DIMACS member), Salil Vadhan (DIMACS visitor) and Avi Wigderson began a collaboration on this problem, which led to a remarkably elementary and elegant combinatorial construction of expanders. This construction is based on the iteration of a new type of graph product, the Zig-Zag product, which allows one to preserve expansion properties while retaining small degree. These results were presented by Wigderson at the SYCI workshop on "Intrinsic Complexity of Computation." This work was continued in a later paper (with the same authors, and Michael Capalbo (DIMACS-IAS postdoc)). In this work, the authors introduced a generalization of expanders called *randomness conductors* which are functions that have certain entropy preserving characteristics that make them useful in constructions of pseudorandom objects.

  > O. Reingold, S. Vadhan, and A. Wigderson, Entropy Waves, the Zig-Zag product and New constant-degree expanders and extractors, DIMACS Technical Report 2001-09, February 2001. To appear in Annals of Mathematics.

  > M. Capalbo, O. Reingold, S. Vadhan, and A. Wigderson, Randomness conductors, and expansion beyond the degree/2 barrier, preprint.

- **Random projections and geometric algorithms**

  One of the key algorithmic tools that has emerged over the past few years, for dealing with a number of difficult computational problems, is the "random projection" method. This method applies in a situation where the input can be modeled by points in a high dimensional Euclidean space. The method consists of selecting a low dimensional subspace at random and projecting the points down to that space, and extracting information from this low dimensional representation.

  Under the auspices of the special year, Santosh Vempala is completing a monograph explaining this technique, and giving a variety of examples of it. The volume will be published in the DIMACS-AMS series.

  S. Vempala, Random Projections and Geometric Algorithms, in preparation.

- **Private information retrieval**

  A private information retrieval protocol enables a user to retrieve a data item from a database while hiding the identity of the item being retrieved. In a t-private, k-server PIR protocol, the database is replicated among k servers and the user's privacy is protected from collusion by up to t servers. The main cost measure of such protocols is the communication complexity of retrieving a single bit of data.

  DIMACS postdoc Yuval Ishai and DIMACS visitor (and former postdoc) Amos Beimel developed a general construction for such protocols in the information theoretic setting. This solution builds on a communication protocol due to Babai, Kimmel and Lokam, and unifies and simplifies many of the previous constructions of such protocols.

  A. Beimel and Y. Ishai, Information-theoretic private information retrieval: a unified construction. Proc. ICALP, 2001, 912-926.

- **Randomizing polynomials**

  DIMACS postdoc Yuval Ishai and DIMACS member Eyal Kushilevitz introduced a new representation of functions called "randomizing polynomials", and showed that with this representation any function can be represented by a degree 3 polynomial. This is applied to obtain improved bounds on the number of rounds needed to securely compute functions in a distributed setting.

  Y. Ishai and E. Kushilevitz, Randomizing polynomials: A new representation with applications to round-efficient secure computation, Symp. Foundations of Computer Science, 2000, 294-304.

- **Directed cuts and multicommodity flow**

  The multicommodity flow and its dual, the multicut problem are two of the central problems in graph algorithms. In the latter problem we have a graph G with costs on the edges and k pairs of vertices and we wish to find the set of edges of total cost that disconnect each of the k pairs of vertices.

  The problem is NP complete. One approach to approximating the solution is to look at the linear programming relaxation of the problem. In the undirected case it was proved that this relaxation always gives an answer that is at most a $\log k$ factor smaller than the minimum multicut.

  However, the situation for directed graphs has been much harder to deal with. DIMACS member Michael Saks, and postdocs Alex Samorodnitsky and Leonid Zosin gave an example of an instance of k-multicut where the ratio between the best integer solution and the best fractional solution is k.

  M. Saks, A. Samorodnitsky and L. Zosin, A lower bound on the integrality gap for minimum multicut for directed graphs, Combinatorica, to appear.

- **Secret Sharing and hypergraph decomposition**

  Secret sharing schemes are important primitives for the design of general cryptographic protocols. Such a scheme is a protocol that allows one participant (the dealer) to divide information among many other participants in such a way that the dealer's information can be reconstructed from all of the shares together, but no small set of the participants can learn anything about the dealer's information from their shares.

DIMACS member Giovanni Di Crescenzo and DIMACS student visitor Clemente Galdi used a technique called hypergraph decomposition to construct much more efficient protocols for certain classes of network access structures: hyperpaths, hypercycles, hyperstars and hypertrees).

G. Di Crescenzo and C. Galdi, Secret sharing and hypergraph decomposition

- **Minimal complete primitives for secure multi-party computation**

  The study of minimal cryptographic primitives needed to implement secure computation among two or more players is a fundamental question in cryptography. The issue of complete primitives for the case of two players has been thoroughly studied. However, in the multi-party setting, when there are $n > 2$ players and t of them are corrupted, the question of what are the simplest complete primitives remained open for $t \geq n/3$.

  Dimacs members Juan Garay and Rafail Ostrovsky worked with DIMACS student visitor Matthias Fitzi and U. Maurer to initiate an investigation of this question. They looked for complete primitives *of minimal cardinality* for secure multi-party computation. The cardinality issue (number of players accessing the primitive) is essential in settings where the primitives are implemented by some other means, and the simpler the primitive the easier it is to realize it. They showed that their primitives are complete and of minimal cardinality possible.

  M. Fitzi, J. Garay, U. Maurer, and R. Ostrovsky, Minimal complete primitives for secure multi-party computation, Proc. Advances in Cryptology (CRYPTO), 2001.

- **Pseudorandom generators in propositional proof complexity**

  Pseudorandom generators play a central role in theory of computing, both in the study of how randomness is used in computation, and in cryptography. DIMACS visitor Alexander Razborov, working with Michael Alekhnovich, Eli Ben Sasson and Avi Wigderson initiated a study of such generators from the perspective of propositional proof complexity. They established that under certain circumstances, these generators are hard for such proof systems as Resolution, Polynomial Calculus and Polynomial Calculus with Resolution.

  M. Alekhnovich, E. Ben-Sasson, A. Razborov and A. Wigderson, Pseudorandom generators in propositional proof complexity, preprint. Electronic Colloquium on Computational Complexity (2000) (see also Proc. of the 41st IEEE FOCS). Submitted for journal publication.

4 Postdoctoral Fellows and Students

One of the goals of this project was to involve outstanding junior people (students and postdoctoral fellows) in the research. Postdoctoral fellows performed their own research under the mentorship of permanent members of DIMACS. Local graduate students attended workshops and engaged in small special year research projects under faculty supervision. Non-local graduate students participated as workshop attendees and as visitors, working on research projects with DIMACS members, postdocs, and other visitors. Undergraduates participated in the research through our undergraduate research program, mentored by DIMACS faculty and postdoctoral fellows.

- **Postdoctoral Associates:**

  – **Yuval Ishai**
  Current position: AT&T Labs - Research

  – **Ashwin Nayak**
  Current Position: Postdoctoral Fellow, California Institute of Technology

- **Nicolas Schabanel**
  Current position: CNRS, Laboratoire de l'Informatique du Parallelisme, Ecole Normale Superieure de Lyon
- **Dieter van Melkebeek**
  Current position: Assistant Professor, University of Wisconsin - Madison, Department of Computer Science
- **Mahesh Viswanathan**
  Current position: Assistant Professor, University of Illinois at Urbana-Champaign, Department of Computer Science

- **Local Graduate students:**
  - **Thomas Davoine**, RUTCOR, Current Position: Consultant, EuroGroup Consulting, Paris, France
  - **Khaled Elbassion**, Computer Science, current Graduate Student
  - **Ayman Khalfalah**, Computer Science, Current Position: Senior System Engineer, Panasonic
  - **Michal Koucky**, Computer Science, current Graduate Student
  - **Xiaoyong Li**, Mathematics, current Graduate Student
  - **Sachin Lodha**, Computer Science, current Graduate Student
  - **Mikhail Nediak**, RUTCOR, current Graduate Student
  - **Clifford Smyth**, Mathematics, Current Position: Institute for Advanced Study (1 year visiting position), then Assistant Professor, Carnegie Mellon University (3 year position)
  - **Amy Stern**, Mathematics, current Graduate Student
  - **Xiaodong Sun**, Mathematics, current Graduate Student
  - **Pierangela Veneziani**, RUTCOR, current Graduate Student
  - **Yi Zhao**, Mathematics, Current Position: Instructor, Department of Mathematics, Rutgers University
  - **Igor Zverovich**, RUTCOR, current Graduate Student
- **Non-local Graduate Students:**
  - **Luis Filipe Coelho Antunes**, LIACC - Centro de Informatica da UP
  - **Albert Atserias**, Universitat Politecnica de Catalunya
  - **Michael Elkin**, Weizmann Institute of Science
  - **Matthias Fitzi**, Institut für Theoretische Informatik
  - **Clemente Galdi**, University of Salerno
  - **Dror Rawitz**, Technion
  - **Pranab Sen**, Tata Institute for Fundamental Research
  - **Adam Smith**, Massachusetts Institute of Technology
- **Undergraduate Students:**
  - **Rodolfo Perez**, Harvard College
  - **Nicolas Ross**, University of California-Berkeley

5 Visitors

The special year involved scientists from numerous institutions in numerous countries. There were hundreds of attendees at our workshops, coming from a variety of types of institutions and disciplines. The resulting collaborations also involved individuals from many institutions in many countries.

A large number of individuals also participated as "visitors," coming for a visit of a few days to a few months. Here is a list of visitors:

- **Noga Alon**; Tel-Aviv University
  Dates: 10/6/1999 - 10/18/1999
- **Albert Atserias**; Universitat Politecnica de Catalunya
  Dates: 12/6/2000 - 12/9/2000
- **Yossi Azar**; Tel Aviv University
  Dates: 2/18/2000 - 2/24/2000
- **Reuven Bar-Yehuda**; Technion
  Dates: 2/17/2000 - 2/26/2000
- **Howard Barnum**; University of Bristol
  Dates: 6/1/2001 - 8/31/2001
- **Richard Beigel**; University of Illinois at Chicago
  Dates: 8/1/1999 - 9/1/2000
- **Amos Beimel**; Ben Gurion University
  Dates: 8/11/2000 - 8/19/2000
- **Amos Beimel**; Ben Gurion University
  Dates: 6/22/2001 - 6/29/2001
- **Andreas Brandstaedt**; University of Rostock
  Dates: 2/1/2001 - 2/15/2001
- **Joseph Cheryan**; University of Waterloo
  Dates: 2/23/2000 - 3/3/2000
- **Dong P. Chi**; Seoul National University
  Dates: 1/14/2001 - 2/4/2001
- **Janos Csirik**; University of Szeged
  Dates: 7/5/2001 - 7/16/2001
- **Paolo D' Arco**; University of Salerno
  Dates: 6/18/2001 - 6/24/2001
- **Michael Elkin**; Weizmann Institute of Science
  Dates: 9/16/2001 - 9/21/2001
- **Guy Even**; Tel Aviv University
  Dates: 8/1/1999 - 8/31/1999
- **Uri Feige**; Weizmann Institute of Science
  Dates: 2/19/2000 - 3/3/2000
- **Matthias Fitzi**; Institut für Theoretische Informatik
  Dates: 8/24/2001 - 8/31/2001
- **Ari Freund**; Technion
  Dates: 7/17/2000 - 8/11/2000

- **Anna Gal**; University of Texas at Austin
  Dates: 5/8/2000 - 6/10/2000
- **Clemente Galdi**; University of Salerno
  Dates: 8/5/2000 - 8/14/2000
- **Clemente Galdi**; University of Salerno
  Dates: 4/30/2001 - 9/26/2001
- **Vince Grolmusz**; Eötvös University
  Dates: 3/17/2000 - 4/16/2000
- **Vladimir Gurvich**; Russian Academy of Science
  Dates: 7/1/2001 - 8/31/2001
- **Eran Halperin**; Tel Aviv University
  Dates: 1/16/2001 - 1/16/2001
- **Johan Hastad**; Royal Institute of Technology
  Dates: 2/13/2000 - 2/24/2000
- **Marek Karpinski**; University of Bonn
  Dates: 2/19/2000 - 3/31/2000
- **Marek Karpinski**; University of Bonn
  Dates: 9/15/2000 - 10/15/2000
- **Claire Kenyon**; Laboratoire de recherche en informatique
  Dates: 4/9/2000 - 4/23/2000
- **Michael Krivelevich**; Tel Aviv University
  Dates: 9/24/2000 - 10/7/2000
- **Felix Lazebnik**; University of Delaware
  Dates: 9/1/2000 - 12/31/2000
- **Satya (Satyanarayana) Lokam**; Loyola University - Chicago
  Dates: 3/2/2000 - 3/10/2000
- **Satya (Satyanarayana) Lokam**; Loyola University - Chicago
  Dates: 5/5/2000 - 5/19/2000
- **Satya (Satyanarayana) Lokam**; Loyola University - Chicago
  Dates: 7/3/2000 - 7/16/2000
- **Ashwin Nayak**; University of California at Berkeley
  Dates: 10/20/1999 - 10/21/1999
- **Ashwin Nayak**; California Institute of Technology
  Dates: 3/26/2001 - 4/4/2001
- **Ashwin Nayak**; California Institute of Technology
  Dates: 5/21/2001 - 5/25/2001
- **Ramamohan (Mohan) Paturi**; University of California - San Diego
  Dates: 11/7/1999 - 12/3/1999
- **Giuseppe (Pino) Persiano**; Universit'a di Salerno
  Dates: 8/2/2000 - 9/3/2000
- **Giuseppe (Pino) Persiano**; Universit'a di Salerno
  Dates: 7/15/2001 - 8/31/2001

- **Erez Petrank**; Technion
Dates: 7/24/2000 - 8/4/2000
- **Toni Pitassi**; University of Arizona
Dates: 10/12/1999 - 10/15/1999
- **Yuval Rabani**; Technion
Dates: 2/13/2000 - 2/24/2000
- **Dieter Rautembach**; Lehrstuhl II für Mathematik
Dates: 11/1/1999 - 11/30/1999
- **Dror Rawitz**; Technion
Dates: 7/31/2001 - 8/10/2001
- **Ran Raz**; The Weizmann Institute of Science
Dates: 10/6/1999 - 10/22/1999
- **Alexander Razborov**; Steklov Mathematical Institute
Dates: 9/29/1999 - 2/28/2000
- **Bruce Reed**; University of Toronto
Dates: 11/1/1999 - 11/30/1999
- **Pranab Sen**; Tata Institute of Fundamental Research
Dates: 11/16/2000 - 12/11/2000
- **Miklos Simonovits**; Mathematical Institute of the Hungarian Academy of Sciences
Dates: 6/10/2000 - 6/29/2000
- **Jacques Stern**; École Normale Supérieure
Dates: 3/19/2000 - 3/23/2000
- **Ram Swaminathan**; (formerly) Bell Labs
Dates: 4/1/2000 - 6/19/2000
- **Gabor Tardos**; Eötvös Loránd Tudományegyetem
Dates: 10/23/1999 - 11/19/1999
- **Tatsuie Tsukiji**; Nagoya University
Dates: 2/25/2000 - 2/29/2000
- **Salil Vadhan**; MIT Laboratory for Computer Science
Dates: 10/12/1999 - 10/22/1999
- **Vinodchandran Variyam**; University of Aarhus / BRICS
Dates: 4/10/2000 - 4/30/2000
- **David Zuckerman**; University of California, Berkeley & University of Texas at Austin
Dates: 10/12/1999 - 10/22/1999

6 Publications

6.1 Journal Publications

The following papers have been reported to us as having been inspired by the special year. There are certainly many more.

- W. Aiello, Y. Ishai, and O. Reingold, Priced Oblivious Transfer: How to Sell Digital Goods, in Proc. of EUROCRYPT '01 (2001)

- M. Alekhnovich, E. Ben-Sasson, A. Razborov, and A. Wigderson, Pseudorandom Generators in Propositional Proof Complexity, Electronic Colloquium on Computational Complexity (2000) (see also Proc. of the 41st IEEE FOCS).
- A. Ambainis, E. Bach, A. Nayak, A. Vishwanath, and J. Watrous, One-dimensional quantum walks, Proc. 33rd ACM STOC, pages 37-49 (2001).
- A. Ambainis, H. Buhrman, W.I. Gasarch, B. Kalyanasundaram and L. Torenvliet, The communication complexity of enumeration, elimination and selection. Accepted for publication in Journal of Computer and System Sciences.
- A. Amir and R. Beigel, W. Gasarch, Some connections between bounded query classes and non-uniform complexity, Electronic Colloquim on Computational Complexity (ECCC)(24): (2000).
- L. Antunes, L. Fortnow, D. van Melkebeek, Computational depth, in Proc. 16th IEEE Conf. on Computational Complexity, 266–273 (2001).
- Y. Bartal, M. Charikar, and D. Raz, Approximating min-sum k-clustering in metric spaces, Proc. 33rd STOC, pp. 11-20 (2001).
- P. Beame, M. Saks, X. Sun and E. Vee, Super-linear time-space tradeoff lower bounds for randomized computation, Proc. 41st IEEE Symp. on Foundations of Computer Science, pp. 169-179 (2000). An expanded version is in preparation.
- R. Beigel, N. Alon, M.S. Apaydin, L. Fortnow, and S. Kasif, An optimal procedure for gap closing in whole genome shotgun sequences, in the proceedings of the 5th International Conference on Computational Molecular Biology (RECOMB), ACM, pp. 22-30 (2001).
- A. Beimel and Y. Ishai, Information-Theoretic Private Information Retrieval: A Unified Construction, in Proc. of ICALP '01 (2001).
- A. Beimel and Y. Ishai, On the Power of Nonlinear Secret-Sharing, in Proc. of the Computational Complexity Conference (CCC) '01 (2001)
- A. Beimel, Y. Ishai, and T. Malkin, Reducing the Servers' Computation in Private Information Retrieval: PIR with Preprocessing, in Proc. of CRYPTO '00. (2000)
- J. Bierbrauer and H. Schellwat, Weakly biased arrays, weakly dependent arrays and error-correcting codes. (A. Barg, S. Litsyn, eds.) AMS-DIMACS Series, Vol. 56, pp. 33-46 (2001)
- J. Bierbrauer and H. Schellwat, Almost independent and weakly biased arrays: efficient constructions and cryptologic applications, Advances in Cryptology - CRYPTO 2000 (M. Bellare, ed.), Lecture Notes in Computer Science **1880** pp. 533-543 (2000).
- B. Bollig, M. Sauerhoff and I. Wegener, On the non-approximability of Boolean functions by OBDDs and Read-k-Times branching programs, in Proc. of IEEE Conference on Computational Complexity, pp. 172-187 (2001).
- H. Buhrman, S. Fenner, L. Fortnow, D. van Melkebeek, Optimal proof systems and sparse sets. Proceedings of the 17th Annual GI/AFCET Symposium on Theoretical Aspects of Computer Science, Lille, France, February 2000. Lecture Notes in Computer Science, volume 1770, Springer, Berlin, pages 407-418 (2000).
- R. Canetti, I. Damgard, S. Dziembowski, Y. Ishai, and T. Malkin, On Adaptive vs. Non-adaptive Security of Multiparty Protocols, in Proc. of EUROCRYPT '01 (2001).
- R. Canetti, R. Kumar, Y. Ishai, M. Reiter, R. Rubinfeld, and R. Wright, Private Function Evaluation with Sublinear Communication, in Proc. of PODC '01, pp. 293-302 (2001).
- J. Cheriyan, H. Karloff, Y. Rabani, Approximating directed multicuts, Proc. 42nd IEEE FOCS (2001).

- M. Dyer, L.A. Goldberg, C. Greenhill, G. Istrate and M. Jerrum, Convergence of the Iterated Prisoner's Dilemma game, to appear in Combinatorics, Probability and Computing (2001).
- O.V. Goldreich and L.V. Trevisan, Three theorems regarding testing graph properties, Proc. of the 42nd FOCS, pp. 460-469 (2001).
- U. Feige, Coping with the NP-hardness of the graph bandwidth problem, in Proc. SWAT 2000, Magnus Haldorsson (Ed.), Lecture Notes in Computer Science 1851, Springer, pages. 10–19.
- J. Feigenbaum, Y. Ishai, T. Malkin, K. Nissim, M. Strauss, and R. Wright, Secure Multiparty Computation of Approximations, in Proc. of ICALP '01 (2001).
- L. Fortnow and D. van Melkebeek, Time-space tradeoffs for nondeterministic computation, Proc. 15th IEEE Conf. on Computational Complexity, 2–13 (2000).
- L. Fortnow, Diagonalization. Bulletin of the European Association for Theoretical Computer Science, 71:102-112, Computational Complexity Column (June 2000).
- R. Gennaro, Y. Ishai, E. Kushilevitz, and T. Rabin, The Round Complexity of Verifiable Secret-Sharing and Secure Multicast, in Proc. of STOC '01 (2001).
- J. Gramm, E. Hirsch, R. Niedermaeier, P. Rossmanith, New worst-case upper bounds for MAX-2-SAT with application to MAX-CUT, Electronic Colloquim on Computational Complexity (ECCC)(37) (2000). Presented at SAT 2000, Renesse, The Netherlands, May 2000. A revised version to appear in Discrete Applied Mathematics.
- T. Hayes, S. Kutin and D. van Melkebeek, On the quantum black-box complexity of majority, to appear in Algorithmica.
- Y. Ishai and E. Kushilevitz, Randomizing Polynomials: A New Representation with Applications to Round-Efficient Secure Computation, in Proc. of FOCS '00 (2000)
- K. Iwama, Y. Okabe and T. Takase, Separating oblivious and non-oblivious BPs, Proc. COCOON01 (LNCS2108), pp. 28-38 (2001).
- K. Iwama and S. Tamaki, Exploiting partial knowledge of satisfying assignments, Proc. WAE01 (LNCS2141), pp. 118-128 (2001).
- H. Klauck, A. Nayak, A. Ta-Shma and D. Zuckerman, Interaction in quantum communication and the complexity of set disjointness, Proc. 33rd ACM STOC, ACM Press, pages 124 - 133 (2001).
- F. Lazebnik and D. Mubayi, New lower bounds for Ramsey numbers of graphs and hypergraphs, Advances in Applied Mathematics, to appear.
- M. Parnas, D. Ron, and A. Samorodnitsky, Proclaiming dictators and juntas or testing Boolean formula, Proceedings of RANDOM 01 (2001).
- O. Reingold, S. Vadhan, and A. Wigderson, Entropy Waves, the Zig-Zag Graph Product, and New Constant-Degree Expanders and Extractors, in Proceedings of the 41st Annual Symposium on Foundations of Computer Science, IEEE, pp. 3-13 (2000). Journal version accepted to Annals of Mathematics.
- M. Saks, A. Samorodnitsky and L. Zosin, A Lower Bound on the Integrality Gap for Minimum Multicut for Directed Graphs, Combinatorica, to appear.
- Y. Shavitt, X. Sun, A. Wool, and B. Yener, Computing the Unmeasured: An Algebraic Approach to Internet Mapping, in Proceedings of IEEE Infocom 2001, pages 1646-1654.
- L. Trevisan and S. Vadhan, Extracting Randomness from Samplable Distributions, in Proceedings of the 41st Annual Symposium on Foundations of Computer Science, IEEE (2000).
- D. van Melkebeek, Time-space lower bounds for satisfiability, Bulletin of the European Assoc. for Theor. Computer Science, 73 57–77 (2001).

6.2 Books or other non-periodicals

- S. Vempala, Random Projections and Geometric Algorithms, in preparation.

6.3 DIMACS Technical Reports

- 1999-48: *Optimal Proof Systems and Sparse Sets* by Harry Buhrman, Steve Fenner, Lance Fortnow and Dieter van Melkebeek.
- 2000-11: *A Note on Set Systems with no Union of Cardinality 0 Modulo m* by Vince Grolmusz.
- 2000-14: *An Inequality for Polymatroid Functions and its Applications* by E. Boros, K. Elbassioni, V. Gurvich and L. Khachiyan.
- 2000-21: *An Efficient Incremental Algorithm for Generating All Maximal Independent Sets for Hypergraphs of Bounded Dimension* by E. Boros, K. Elbassioni, V. Gurvich and L. Khachiyan.
- 2000-28: *Explicit Interpolation Sets Using Perfect Hash Families* by Xiaodong Sun.
- 2000-36: *Interaction in Quantum Communication and the Complexity of Set Disjointness* by Ashwin Nayak, Amnon Ta-Shma and David Zuckerman.
- 2000-43: *Quantum Walk on the Line* by Ashwin Nayak and Ashvin Vishwanath.
- 2000-45: *On the Ratio of the Stability Number and the Domination Number* by I. E. Zverovich and I. I. Zverovich.
- 2001-03: *Constructing Set-Systems with Prescribed Intersection Sizes* by Vince Grolmusz.
- 2001-04: *Set-Systems with Restricted Multiple Intersections and Explicit Ramsey Hypergraphs* by Vince Grolmusz.
- 2001-06: *Weighted Well-covered Graphs and Complexity Questions* by I. E. Zverovich.
- 2001-07: *Finding a Maximum Stable Set in Pentagraphs* by I. E. Zverovich and I. I. Zverovich.
- 2001-09: *Entropy Waves, the Zig-Zag Graph Product, and New Constant-Degree Expanders and Extractors* by Omer Reingold, Salil Vadhan, and Avi Wigderson.
- 2001-11: *k-wise Set-Intersections and k-wise Hamming-Distances* by Vince Grolmusz and Benny Sudakov.
- 2001-12: *On Generating all Minimal Integer Solutions for a Monotone System of Linear Inequalities* by E. Boros, K. Elbassioni, V. Gurvich, L. Khachiyan and K. Makino.
- 2001-35: *Secret Sharing and Hypergraph Decomposition* by Giovanni Di Crescenzo and Clemente Galdi.
- 2001-36: *On a Tiling Conjecture of Komlos for 3-Chromatic Graphs* by A. Shokoufandeh and Y. Zhao. Submitted to Discrete Math.
- 2001-38: *On a conjecture of Loebl* by Y. Zhao.
- 2001-41: *1.375-Approximation Algorithm for Sorting by Reversals* by Piotr Berman, Sridhar Hannenhalli, and Marek Karpinski.
- 2001-42: *Efficient Amplifiers and Bounded Degree Optimization* by Piotr Berman and Marek Karpinski.

6.4 Other Reports and Preprints

The following papers have been reported to us as having been inspired by the special year.

- P. Beame, Erik Vee, Time-Space tradeoffs, multiparty communication protocols and nearest neighbor problems, 2001, preprint.
- R. Beigel and L. Fortnow. Are Cook and Karp ever the same? Technical Report 2001-002, NEC Research Institute, (2001).
- R. Beigel, H. Buhrman, L. Fortnow, L. Longpre, and L. Torenvliet. Enumerations of the Kolmogorov function. Technical Report 2001-004, NEC Research Institute (2001).
- A. Brandstadt, C. Hoang and I. Zverovich, Extension of claw-free graphs and (K1 U P4)-free graphs with substitutions, RUTCOR Research Report 28-2001 (2001).
- A. Brandstadt and V. V. Lozin, On the linear structure and clique-width of bipartite permutation graphs, RUTCOR Research Report 29-2001 (2001).
- M. Capalbo, O. Reingold, S. Vadhan, and A. Wigderson, Randomness conductors, and expansion beyond the degree/2 barrier, preprint.
- T. Davoine, P. Hammer, and B. Vizvari, A Heuristic for Boolean Optimization Problems, Rutcor Research Report 42-2000 (2000).
- G. Di Crescenzo and C. Galdi, Secret Sharing and Hypergraph Decomposition, submitted.
- G. Di Crescenzo, C. Galdi, G. Giammarino and N. Semret, Secret Sharing Schemes for Group Graph, in preparation.
- M. Fitzi and J. Garay, Secure, efficient and processor-optimal strong consensus, submitted.
- N. Maxemchuk, S. Muthukrishnan, B. Badrinath, S. Rajagopalan, F.S. Roberts, N. Schabanel, and M. Viswanathan, Very large scale mobile ubiquitous networking, DIMACS Report, June 29, 2001.
- M. Nediak, A Heuristic Algorithm for Mixed Integer Programming, in preparation.
- M. Nediak, and J. Eckstein, Pivot, Cut, and Dive: A Heuristic for 0-1 Mixed Integer Programming, RUTCOR Research Report 53-2001 (2001). Article submitted to Operations Research.

date of report: 12-1-01