ESPRIT BR Working Group – 7097 (RAND)

Annual Progress Report
1992 / 1993

1 Overview

The research was conducted in all the main research areas of RAND:

(1) Design of Efficient Randomized Algorithms

(2) Foundations of Randomized Complexity

(3) Randomized Approximation Algorithms

(4) Derandomizing Algorithms

(5) Computational Learning Theory

The research on Design of Efficient Randomized Algorithms (Work Area 1) was focussed on design of efficient algorithms for combinatorial and algebraic problems.

The research on Foundations of Randomized Complexity (Work Area 2) was focussed on the problems of separation of randomized time classes, design of pseudorandom generators, and direct interactive protocols for combinatorial enumeration problems.

The research on Randomized Approximation (Work Area 3) and Derandomizing Algorithms (Work Area 4) was concentrated on efficient approximation algorithms for the number of important combinatorial counting problems, as well the uniform and deterministic simulations of general threshold circuits by the majority circuits.

The research activities in Computational Learning Theory (Work Area 5) was mainly concerned with the problems of learning some classes of boolean functions by queries, VC–dimension of polynomials and rational functions, and sparse interpolation.

The 77 research papers resulting from the RAND activities are listed separately in the next section.

2 Research Papers (RAND)

(1) Anan, J.:
A randomised approximation algorithm for counting the number of forests in dense graphs
June 1993

(2) Anan, J.:
The complexity of coefficients of the Tutte polynomial
to be published in *Discrete Math.*

(3) Bampis, E., Haddad, M. E., Manoussakis, Y. and Santha, M.:
PARLE 93: A parallel reduction of Hamiltonian cycle to Hamiltonian path in tournaments
Lecture Notes in Computer Science, Springer Verlag, 1993

(4) Barbaroux, P.:
EUROCRYPT 92: Uniform results in polynomial time security
Lecture Notes in Computer Science, vol. 658, Springer Verlag, 1992, pp. 297–306

(5) Bshouty, N. H., Hancock, T. R., Hellerstein, L. and Karpinski, M.:
An Algorithm to Learn Read–Once Treshold Formulas, and Some Generic Transformations Between Learning Models
Technical Report TR–93–037, International Computer Science Institute, Berkeley, 1993

(6) Bürgisser, P., Karpinski, M. and Lickteig, T.:
On Randomized Algebraic Test Complexity
to appear in *Journal of Complexity, 1993*

(7) Chen, Jingsen:
Constructing Priority Queues and Deques Optimally in Parallel
Proceedings of the 12^{th} IFIP World Computer Congress, Vol. 1, Madrid, 1992, pp. 275–283

(8) Cowling, P.:
Strong total chromatic numbers of complete hypergraphs
British Comb. Conference, Keele, 1993, submitted to *Discrete Math.*

(9) Dahlhaus, E., Karpinski, M. and Kelsen, P.:
An Efficient Parallel Algorithm for Computing a Maximal Independent Set in a Hypergraph of Dimenssion 3
Information Processing Letters, vol. 42, 1992, pp. 309–313

(10) Diaz, J., Rougemont, M. de and Santha, M.:
On the interactive complexity of graph enumeration problems
RAND International Workshop: Randomized Algorithms, March 1993

(11) Dyer, M., Frieze, A. and Jerrum, M.:
Approximately Counting Hamilton Cycles in Dense Graphs
Report ECS–LFCS–93–259, Department of Computer Science, University of Edinburgh, April 1993
submitted to *IEEE Symposium on Foundations of Computer Science*

(12) Fernandez de la Vega, W. and Maftouhi, H. E.:
Almost all satisfiable 3–CNF formulas have exponentially many models
Jerusalem Combinatorics Conference, May 1993

(13) Fernandez de la Vega, W. and Maftouhi, H.E.:
On the threshold for the almost sure satisfiability of a random set of 3–clauses
RAND International Workshop: Randomized Algorithms, March 1993.

(14) Fernandez de la Vega, W. and Manoussakis, Y.:
Grids in random graphs
to appear in *Random structures and algorithms, 1993*

(15) Fernandez de la Vega, W. and Santha, M.:
Average case analysis of the merging algorithm of Hwang and Lin
Fifth Franco–Japanese Days on Combinatorics and Optimization, Kyoto, October 1992

(16) Garrido, O., Lingas, A., Jarominek, J. and Rytter, W.:
A Simple Randomized Parallel Algorithm for Maximal f–Matchings
Proceedings of LATIN '92, Lecture Notes in Computer Science, vol. 583, Springer Verlag, 1992, pp. 165–176

(17) Gathen, J. von zur, Karpinski, M. and Sharlinski, I.:
Counting Curves and Their Projections
Proceedings of the 25^{th} ACM STOC, 1993, pp. 805–812

(18) Goldberg, P. and Jerrum, M.:
Bounding the Vapnik–Chervonenkis Dimension of Concept Classes Parameterized by Real Numbers (Extended Abstract)
NEC Research Institute Technical Report 93–028–3–9004–1.
to appear in *Proceedings of the ACM Symposium on Computational Learning Theory, July 1993*

(19) Goldberg, P., Jerrum, M., Leighton, T. and Rao, S.:
A Doubly Logarithmic Communication Algorithm for the Completely Connected Optical Communication Parallel Computer
NEC Research Institute Technical Report 93–016–3–0054–3.
to appear in *Proceedings of the ACM Symposium on Parallel Algorithms and Architectures, July 1993*

(20) Goldmann, M. and Karpinski, M.:
Simualting Threshold Circuits by Majority Circuits
Proceedings of the 25^{th} ACM STOC, 1993, pp. 551–560

(21) Grigoriev, D. and Karpinski, M.:
A Zero–Test and an Interpolation Algorithm for the Shifted Sparse Polynomials
Proceedings of the AAECC 93, Lecture Notes in Computer Science, vol. 673, Springer Verlag, 1993, pp. 162–169

(22) Grigoriev, D., Karpinski, M. and Odlyzko, A.
Short Proofs for Nonindivisibility of Sparse Polynomials under the Extended Riemann Hypothesis
Proceedings of the ACM ISSAC 92, 1992, pp. 117–122

(23) Grigoriev, D., Karpinski M. and Singer, M.:
Interpolation of Sparse Rational Functions without Knowing Bounds on Exponents
to appear in *SIAM Journal of Computing, 1993*

(24) Gustedt, J., Steger, A.:
Testing hereditary properties efficiently
Forschungsinstitut f"ur Diskrete Mathematik, Universität Bonn, 1993

(25) Hougardy, S., Prömel, H. J. and Steger, A.:
$NP = PCP$ *and its consequences for approximation algorithms*
Forschungsinstitut f"ur Diskrete Mathematik, Universität Bonn 1993,
to appear in *Trends in Discrete Mathematics, (W. Deuber, H. J. Prömel, B. Voigt, eds.), North Holland*

(26) Hundack, C., Prömel, H. J. and Steger, A.:
A random graph problem
Forschungsinstitut f"ur Diskrete Mathematik, Universität Bonn 1993.
to appear in *Proceedings of the Cambridge Combinatorial Conference in Honour of Paul Erdős on his* 80^{th} *Birthday, (B. Bollobás, ed.)*

(27) Jerrum, M.:
An Analysis of a Monte Carlo Algorithm for Estimating the Permanent
Proceedings of the 3^{rd} Conference on Integer Programming and Combinatorial Optimization, CORE, Louvain–la–Neuve, Belgium, April 1993, pp. 171–182

(28) Jerrum, M.:
Large cliques elude the Metropolis process
Random Structures and Algorithms, vol. 3, 1992, pp. 347–359

(29) Jerrum, M.:
Review of *Probabilistic analysis of packing and partitioning algorithms* by E. G. Coffman jr. and G. S. Lueker
The Annals of Probability, vol. 20, 1992, pp. 2164–2167

(30) Jerrum, M., McKay, B. and Sinclair, A.:
When is a Graphical Sequence Stable?
Random Graphs, vol. 2, (A. Frieze and T. Luczak, eds), Wiley 1992, pp. 101–115

(31) Jerrum, M. and Sorkin, G.:
Simulated Annealing for Graph Bisection
Report ECS–LFCS–93–260, Department of Computer Science, University of Edinburgh, April 1993
submitted to *Symposium on Foundations of Computer Science*

(32) Jerrum, M. and Vazirani, U.:
A mildly exponential approximation algorithm for the permanent
Proceedings of the 33^{rd} Annual IEEE Conference on Foundations of Computer Science, IEEE Computer Society Press, October 1992, pp. 320–326

(33) Karpinski, M. and Luby, M.:
Approximating the Number of Zeros of a GF[2] Polynomial
J. of Algorithms, vol. 14, 1993, pp. 280–287

(34) Karpinski, M. and Verbeek, R.:
On Randomized versus Deterministic Computation
Proceedings of the 20^{th} ICALP, Lecture Notes in Computer Science, vol. 700, Springer Verlag, 1993, pp. 227–240

(35) Karpinski, M. and Werther, T.:
VC Dimension and Uniform Learnability of Sparse Polynomials and Rational Functions
to appear in *SIAM Journal of Computing, no. 22, vol. 6, 1993*

(36) Kenyon, C., Randall, D. and Sinclair, A.:
Matchings in Lattice Graphs
Proceedings of the 25^{th} ACM Symposium on Theory of Computing, San Diego, May 1993, pp. 738–746

(37) Lickteig, L. and Werther, K.:
Optimal Computation of the Complex Square Root over the Reals
in preparation

(38) Lingas, A. and Klein, R.:
A Linear–time Randomized Algorithm for the Bounded Voronoi Diagram of a Simple Polygon
Proceedings of the ACM Symposium on Comnputational Geometry, San Diego, 1993

(39) Lingas, A. and Klein, R.:
A Note on Generalizations of Chew's Randomized Algorithm for the Voronoi Diagram of a Convex Polygon
to appear in *Proceedings of the 5^{th} Canadian Conference on Computational Geometry*, Waterloo, 1993

(40) Luby. M., Sinclair, A. and Zuckerman, D.:
Optimal Speedup of Las Vegas Algorithms
to appear in Proceedings of the 2^{nd} Israel Symposium on Theory of Computing and Systems, Jerusalem, June 1993

(41) McDiarmid, C. J. H.:
A random recolouring method for graphs and hypergraphs
submitted

(42) McDiarmid, C. J. H.:
On the correlation inequality of Farr
Combinatorics, Probability and Computing, vol. 1, 1992, pp. 157–160

(43) McDiarmid, C. J. H.:
Probability modelling and optimal location of a travelling salesman
Journal of Operational Research Society, vol. 43, 1992, pp. 533–538

(44) McDiarmid, C. J. H. and Chvátal, V.:
Small transversals in hypergraphs
RUTCOR Research Report # 26–88, 1988, Combinatorica, no. 12, vol. 1, 1992, pp. 19–26

(45) McDiarmid, C. J. H. and Edwards, K.:
New upper bounds for harmonious colourings
to appear in *J. Graph Theory*

(46) McDiarmid, C. J. H. and Edwards, K.:
The Complexity of harmonious colouring for trees
submitted

(47) McDiarmid, C. J. H. and Hayward, R.:
Large deviations for Quicksort
to appear

(48) McDiarmid, C. J. H. and Hayward, R.:
Strong concentration for quicksort
Proceedings of the 3^{rd} Annual ACM–SIAM Symposium on Discrete Algorithms (SODA), 1992, pp. 414–421

(49) McDiarmid, C. J. H. and Ramirez–Alfonsin, J.:
Sharing jugs of wine
to appear in *Discrete Mathematics*

(50) McDiarmid, C. J. H. and Reed, B.:
On total colourings of graphs
Journal of Combinatorial Theory, vol. 57, 1993, pp. 122–130

(51) McDiarmid, C. J. H. and Reed, B.:
The strongly connected components of 1–in 1–out
Combinatorics, Probability and Computing, vol. 1, 1992, pp. 265–274

(52) McDiarmid, C. J. H. and Sanchez–Arroyo, A.:
An upper bound for total colouring of graphs
Discrete Mathematics, vol. 111, 1993, pp. 389–392

(53) McDiarmid, C. J. H. and Sanchez–Arroyo, A.:
Total colouring regular bipartite graphs is NP–hard
to appear in *Discrete Mathematics*

(54) McDiarmid, C. J. H., Alon, N. and Reed, B.:
Star arboricity
Combinatorica, vol. 12, no. 4, 1992, pp. 375–380

(55) McDiarmid, C. J. H., Dyer, M. E. and Füredi, Z.:
Volumes spanned by random points in the hypercube
Random Structures and Algorithms, vol. 3, 1992, pp. 91–106

(56) McDiarmid, C. J. H., Frieze, A. and Reed, B.:
On a conjecture of Bondy and Fan
to appear in *Ars Combinatorica*

(57) McDiarmid, C. J. H., Cook, W., Hartmann, M. and Kannan, R.:
On integer points in polyhedra
Combinatorica, vol. 12, no. 1, 1992, pp. 27–37

(58) McDiarmid, C. J. H., Reed, B., Schrijver, A. and Shepherd, B.:
Induced circuits in planar graphs
Centrum voor Wiskunde en Informatica, Amsterdam Technical Report BS–R9106, February 1991
to appear in *J. Combinatorial Theory*

(59) McDiarmid, C. J. H., Reed, B., Schrijver, A. and Shepherd, B.:
Non–interfering network flows
SWAT 1992, Helsinki, Finland, July 1992

(60) Paschos, V. T.:
A $\delta/2$–approximation algorithm for the maximum independent set problem
Information Processing Letters, vol. 44, 1992

(61) Paschos, V. T., Pekergin, F., and Zissimopoulos, V.:
Approximating the optimal solutions of some hard graph problems by a Boltzmann machine
to appear in *Belgian Journal of Operation Research, Statistics and ComputerScience, 1993*

(62) Prömel, H. J. and Steger, A.:
Random l–colorable graph
Forschungsinstitut f"ur Diskrete Mathematik, Universität Bonn 1992

(63) Rabinovich, Y., Sinclair, A. and Wigderson, A.:
Quadratic Dynamical Systems
Proceedings of the 33^{rd} IEEE Symposium on Foundations of Computer Science, Pittsburgh, October 1992, pp. 304–313

(64) Sekine, K.:
The flow polynomial and its computation
M. Sc. thesis, University of Oxford, May 1993

(65) Sinclair, A.:
Algorithms for Random Generation and Counting: A Markov Chain Approach'
monograph in *Progress in Theoretical Computer Science, (R. V. Book ed.), Birkhäuser Boston, December 1992*

(66) Sinclair, A.:.
Improved Bounds for Mixing Rates of Markov Chains and Multicommodity Flow
Combinatorics, Probability and Computing, vol. 1, December 1992, pp. 351–370

(67) Welsh, D. J. A.:
Complexity: Knots Colourings and Counting
London Mathematical Society Lecture Notes, vol. 186, 1993), Cambridge University Press, pp. 176

(68) Welsh, D. J. A. and Schwärzler, W.:
Knots, matroids and the Ising model
Math. Proc. Camb. Phil. Soc., vol. 113, 1993, pp. 107–139

(69) Welsh, D. J. A.:
Percolation in the random cluster process and Q–state Potts model
Journal of Phys. A. (Math and General), vol. 26, 1993, pp. 2471–2483

(70) Welsh, D. J. A.:
Randomised algorithms — zero knowledge proofs
British Association Lecture, August 1992, pp. 10

(71) Welsh, D. J. A.:
The complexity of knots
Annuals of Discrete Mathematics, vol. 55, 1993, pp. 159–172

(72) Welsh, D. J. A. and Oxley, J. G.:
Tutte polynomials computable in polynomial time
Discrete Mathematics, vol. 109, 1992, pp. 185–192

(73) Welsh, D. J. A.:
Knots and braids: Some algorithmic questions
Contemporary Math., vol. 147, 1993, pp. 109–124

(74) Welsh, D. J. A. and Vertigan, D. L.:
The computational complexity of the Tutte plane: the bipartite case
Combinatorics, Probability and Computing, vol. 1, 1992, pp. 181–187

(75) Werther, K.:
The Complexity of Interpolating Sparse Polynomials over Finite Fields
(revised version)
submitted to *AAECC*

(76) Werther, K.:
Generalized Vandermonde Determinants over the Chebyshed Basis
Technical Report TR–93–024, International Computer Science Institute, Berkeley, 1993

(77) Werther, K.:
Sparse Interpolation from Multiple Derivates
Technical Report TR–93–036, International Computer Science Institute, Berkeley, 1993

3 RAND–Workshop, Bonn, March '93 Org.: M. Karpinski, H.–J. Prömel

The Workshop was organized by the ESPRIT BR Workshop Group on Randomized Algorithms (RAND), and the Department of Computer Science of the University of Bonn. It was concerned with the newest development in the design of efficient and pseudo–randomized algorithms, approximation algorithms, circuit design, probabilitic methods and the construction of small sampling spaces as well as with the foundations of complexity theory of randomized computation. Proceedings has appeared as a Research Report No. 8590–CS, Department of Computer Science, University of Bonn (1993).

Talks

- **Ingo Althöfer (Bielefeld):**
Derandomization: Upper and Lower Bounds

  A randomized strategy or a convex combination may be represented by a probability vector $p = (p_1, \ldots, p_m)$. p is called sparse if it has only few positive entries.

  We present the following **Approximation Lemma:**

  Let $A = (a_{ij})$ be an $m \times n$-matrix over the real numbers with $0 \leq a_{ij} \leq 1$ for $1 \leq i \leq m$, $1 \leq j \leq n$. Let $p = (p_1, \ldots, p_m)$ be a probabiblity vector, i.e., $0 \leq p_i$ for i and $\sum_{i=1}^{n} p_i = 1$, and $\epsilon > 0$ any positive constant. Then there exists another probability vector $q = (q_1, \ldots, q_m)$ with at most $k = \lceil \frac{\log 2n}{2\epsilon^2} \rceil$ many positive coordinates q_i such that

  $$\left| \sum_{i=1}^{n} p_i a_{ij} - \sum_{i=1}^{m} q_i a_{ij} \right| \leq \epsilon \quad \text{for all} \quad j = 1, \ldots, n.$$

  More precisely, the probability vector q can be chosen such that $q_i = \frac{k_i}{k}$ with natural numbers k_i for all $i = 1, \ldots, m$.

  The bound k is asymptotically optimal up to the multiplicative constant $4 \log 2 \approx 2.77$.

The Approximation Lemma is applied to matrix games, certain linear programs, and computer chess.

- **Peter Bürgisser, Marek Karpinski & Thomas Lickteig (Bonn):**
  On Randomized Test Complexity

  We investigate the impact of randomization on the complexity of deciding membership in a (semi-)algebraic subset $X \subset \mathbb{R}^{\geqslant}$. Examples are exhibited where allowing for a certain error probability ϵ in the answer of the algorithms the complexity of decision problems decreases. A randomized $(\Omega^k, \{=, \leq\})$-decision tree ($k \subseteq \mathbb{R}$ a subfield) over m will be defined as a pair (T, μ) where μ a probability measure on some $\mathbb{R}^{\kappa}$ and T is a $(\Omega^k, \{=, \leq\})$-decision tree over $m+n$. We prove a general lower bound on the average decision complexity for testing membership in an irreducible algebraic subset $X \subset \mathbb{R}^{\geqslant}$ and apply it to k-generic complete intersection of polynomials of the same degree, extending results of Lickteig, Bürgisser and Lickteig and Bürgisser, Lickteig and Shub. We also give applications to nongeneric cases, such as graphs of elementary symmetric functions, $\mathrm{SL}(m, \mathbb{R})$, and determinant varieties, extending results of Lickteig

- **J. Diaz, M. de Rougemont & Miklos Santha (Paris):**
  On the Interactive Complexity of Graph Enumeration Problems

  We consider three $\#P-$complete enumeration problems on graphs : $s-t$ PATHS, $s-t$ CONNECTEDNESS and $s-t$ RELIABILITY, and give IP protocols for them. If $IP(f(n))$ is the class of languages whose interactive complexity is $O(f(n))$, that is the set of languages which can be accepted by an interactive proof system with $O(f(n))$ number of rounds, then our protocols imply that the interactive complexity of these problems is significantly smaller than what one could get by using generic reductions via Cook's Theorem. Indeed, we show that $s-t$ PATH $\in IP(n)$, $s-t$ CONNECTEDNESS $\in IP(n^2)$, and $s-t$ RELIABILITY $\in IP(n^2)$.

- **Guy Even, Oded Goldreich (Haifa), Michael Luby (Berkeley), Noam Nisan (Jerusalem) & Boban Veličković (Berkeley):**
  "Approximation of general independent distributions"

  In this talk we discuss the problem of efficiently constructing small sample space probability distributions on n Boolean variables which approximate a given independent but not necessarily uniform distribution on n Boolean variables. This problem is frequently encountered in practice, for instance, in the network reliability problem.

  We establish an intimate connection of this question with the problem of construction small discrepancy sets in I^n, the n-dimensional unit cube. This problem has been studied extensively in numerical analysis and essentially optimal constructions have been given in case the dimension is constant.

We present several examples of efficiently constructible small discrepancy sets in I^n of size $\exp(O(\log(n/\epsilon)^2))$, where ϵ is the error paramet

- **W. Fernandez de la Vega & A. El Mafthoui (Paris):**
  On the Treshold for the Almost Sure Satisfiability of a Random Set of 3–Clauses

  Let S be a set of m clauses each containing 3 literals chosen at random in a set $\{p_1, \neg p_1, ..., p_n, \neg p_n\}$ of n propositional variables and their negations. Let c denote the biggest number such that if m and n tend to infinity with $\frac{m}{n} > c$, then the probability that the set S is satisfiable tends to 1 as n tends to infinity. Frieze and Suen have shown recently that c exceeds 3 and it is known that $c \leq \log_{8/7} 2 = 5.19....$ We will present some methods and results concerning better upper bounds for c.

- **Oscar Garrido (Lund), Stefan Jarominek, Wojciech Rytter (Warsaw) & Andrzej Lingas (Lund):**
  A Simple Randomized Parallel Algorithm for Maximal f–Matchings

  We show how to extend the RNC-algorithm for maximal matchings due to Israeli-Itai to compute maximal (with respect to set of edges inclusion) f-matchings. Our algorithm works in $\mathcal{O}(\log^2 n)$ time on an arbitrary CRCW PRAM with a linear number of processors. The algorithm can be used also for multigraphs and then it preserves its complexity.

- **Joachim von zur Gathen (Toronto & Zürich):**
  Probabilistic Methods in Finite Fields

  A polynomial $f \in \mathbb{F}_{\shortparallel}[\frown]$ over a finite field $\mathbb{F}_{\shortparallel}$ is a *permutation polynomial* if and only if the associated mapping $\mathbb{F}_{\shortparallel} \to \mathbb{F}_{\shortparallel}$ is bijective. We present a probabilistic test for this property using essentially $O(n \log q)$ operations in $\mathbb{F}_{\shortparallel}$, where $n = \deg f$; this solves a problem posed by LIDL & MULLEN.

  Furthermore, we give approximation schemes for the size of the image of a polynomial or rational function, and the size of an algebraic curve; these results are joint work with MA and KARPINSKI & SHPARLINSKI, respectively.

- **Jens Gutstedt (Berlin) & Angelika Steger (Bonn):**
  Testing Hereditary Properties efficiently

  The aim of this talk is to develop fast algorithms for hereditary properties that are, while not fast in the worst case, at least fast on average.

  The key observation for such algorithms is that if the probability that a fixed obstruction H op property $\mathcal{E}$ is not contained in the input is low then most possible inputs don't have the property $\mathcal{E}$ and this can be verified by testing for the obstruction H. In this talk we will describe the three parts of such an approach, namely

(1) to show that a fixed obstruction H of a property $\mathcal{E}$ occurs with high probability,

(2) to develop an algorithm that is fast on average and test for a given obstruction H,

(3) to design an exact algorithm for $\mathcal{E}$ whose running time is sufficiently small compared to the probability that the obstruction H does not occur.

We will do that in a general setting, but we will also consider some special examples of combinatorial structures. Among these will be several calsses of graphs equipped with three different relations, namely the induced and weak subgraph relation, and the graph minor relation.

- **Marek Karpinski (Bonn) & Rutger Verbeek (Hagen):**
  On Randomized Versus Deterministic Computation

  In contrast to deterministic or nondeterministic computation, it is a fundamental open problem in randomized computation how to separate different randomized time classes (at this point we do not even know how to separate linear randomized time from $O(n^{\log n})$ randomized time) or how to compare them relative to corresponding deterministic time classes. In another words we are far from understanding the power of *random coin tosses* in the computation, and the possible ways of simulating them deterministically.

  In this paper we study the relative power of linear and polynomial randomized time compared with exponential deterministic time. Surprisingly, we are able to construct an oracle A such that exponential time (with or without the oracle A) is simulated by linear time Las Vegas algorithms using the oracle A. We are also able to prove, for the first time, that in some situations the randomized reductions are exponentially more powerful than deterministic ones (cf. [Adleman, Manders, 1977]).

  Furthermore, a set B is constructed such that Monte Carlo polynomial time (BPP) under the oracle B is exponentially more powerful than deterministic time with nondeterministic oracles. This strengthens considerably a result of Stockmeyer about the polynomial time hierarchy that for some decidable oracle B, $\mathrm{BPP}^B \not\subseteq \Delta_2\mathrm{P}^B$. Under our oracle BPP^B is exponentially more powerful than $\Delta_2\mathrm{P}^B$, and B does not add any power to Δ_2EXPTIME

- **Andrzej Lingas (Lund) & Rolf Klein (Hagen):**
  Linear–Time Randomized Algorithms for Voronoi Diagrams of Simple Polygons

  We present linear-time generalizations of Chew's randomized algorithm for the Voronoi diagram of a convex polygon to include the convex hull of a special polygon in 3D, the Voronoi diagram of a monotone polygon and the bounded Voronoi diagram of a simple polygon.

- **Michael Luby (Berkeley) & Noam Nisan (Jerusalem):**
  A Parallel Approximation Algorithm for Positive Linear Programming

  We introduce a fast parallel approximation algorithm for the positive linear programming optimization problem, i.e., the special case of the linear programming optimization problem where the input constraint matrix and constraint vector constist entirely of positive entries. The algorithm is elementary, and has a simple parallel implementation that runs in polylog time using a linear number of processors.

- **Michael Luby (Berkeley), Seffi (Joseph) Naor & M. Naor (Haifa):**
  On Removing Randomness from a Parallel Algorithm for Minimum Cuts

  The minimum cut problem is the following: partition the vertices of a graph into two disjoint sets so as to minimize the number of edges in the cut, i.e., edges adjacent to vertices that are in different sets. The graph may be weighted, in which case we want to minimize the weight of the edges in the cut. This problem has received much attention in the literature in the last 40 years. It is a fundamental problem in combinatorial optimization and has numerous applications, e.g., network design and reliability, sequencing and scheduling, location theory, partitioning problems, and heuristics for solving integer programming problems. The parallel complexity, however, remained unresolved. Recently, Karger for computing the minimum cut in a graph. This placed the problem in the complexity class RNC.

  We show that a similar algorithm can be implemented using only $O(\log^2 n)$ random bits. We also show that this result holds for computing minimum weight k-cuts, where k is fixed. We view our algorithm as a step towards obtaining a deterministic algorithm for the problem. Alternatively, one can view random bits as a resource (such as time and space), to be used as sparingly as possible, and our result reduces the use of this resource over the algorithm suggested by Karger. Reducing the number of random bits needed in computation is a line that has been explored by many researchers in recent years.

- **Rüdiger Reischuk & Christian Schindelhauer (Darmstadt):**
  Precise Average Case Complexity

  A new definition is given for the average growth of a function $f : \Sigma^* \to \mathbb{N}$ with respect to a probability measure μ on Σ^*. This allows us to define meaningful average case distributional complexity classes for arbitrary time bounds (previously, one could only distinguish between polynomial and superpolynomial growth). It is shown that basically only the ranking of the inputs by decreasing probabilities are of importance.

  To compare the average and worst case complexity of problems we study average case complexity classes defined by a time bound and a bound on the complexity of possible distributions. Here, the complexity is measured

by the time to compute the rank functions of the distributions. We obtain tight and optimal separation results between these average case classes. Also the worst case classes can be embedded into this hierarchy. They are shown to be identical to average case classes with respect to distributions of exponential complexity.

These ideas are finally applied to study the average case complexity of problems in $\mathcal{NP}$. A reduction between distributional problems is defined for this new approach. We study the average case complexity class $\mathcal{A}\sqsubseteq\mathcal{P}$ consisting of those problems that can be solved by DTMs on the average in polynomial time for all distributions with efficiently computable rank function. Fast algorithms are known for some $\mathcal{NP}$–complete problems under very simple distributions. For languages in $\mathcal{NP}$ we consider the maximal allowable complexity of distributions such that the problem can still be solved efficiently by a DTM, at least on the average. As an example we can show that either the satisfiability problem remains hard, even for simple distributions, or $\mathcal{NP}$ is contained in $\mathcal{A}\sqsubseteq\mathcal{P}$, that means every problem in $\mathcal{NP}$ can be solved efficiently on the average for arbitrary not too complex distributions.

- **Eli Shamir (Jerusalem):**
  Information, Prediction and Query by Committee

  A highly desirable goal in approximate learning of concepts by queries is to drive the "prediction error" [exponentially] fast to 0. We show this is achieved if the "expected information-gain" by a query is bounded from 0. "Query by committee" randomized algorithms provide filters which from a random stream of inputs pick up the informative queries. The typical situation we discuss are "generalized perceptrons", i.e. concepts defined by thresholds of smooth functions.

4 Conferences and Workshops attended

- ACM ISSAC '92, Berkeley, July 8, 1992
  (M. Karpinski)
- Dagstuhl Workshop on "Algebraic Complexity and Parallelism", July 1992
  (P. Bürgisser, M. Karpinski, T. Lichteig, K. Werther, T. Werther)
- Dagstuhl Workshop on "Complexity and Realisation of Boolean Functions", August 1992
  (M. Karpinski)
- Dagstuhl Workshop on "Molecular Bioinformatics", September 1992
  (M. Karpinski)

- Dagstuhl Workshop on "Algorithms and Complexity of Continuos Problems", October 1992
  (M. Karpinski)
- IEEE Symposium on Foundations of Computer Science, Pittsburgh, October 1992
  (A. Sinclair)
- Trends in Discrete Mathematics, Bielefeld, October 28 – November 1, 1992
  (S. Hougardy, H.J. Prömel, A. Steger)
- Oberwolfach Tagung on Complexity Theory, Oberwolfach, Germany, November 1992
  (A. Sinclair)
- Oberwolfach Workshop on "Computational Complexity", November 1992
  (M. Karpinski, A. Sinclair)
- DIMACS Workshop on Randomized Algorithms for Combinatorial Optimization, Princeton, USA, February 1993
  (M. Jerrum)
- Bonn Workshop on "Randomized Algorithms" (RAND), March 1993
  (Working Group 7097)
- Cambridge Combinatorial Conference in Honour of Paul Erdős on his 80^{th} Birthday, Cambridge, England, March 22.–26, 1993
  (H. J. Prömel, A. Steger)
- Third Conference on Integer Programming and Combinatorial Optimisation, Erice, Italy, April/May 1993
  (M. Jerrum)
- Leibniz Workshop on "Complexity Theory", Jerusalem, May 1993
  (M. Karpinski)
- ACM Symposium on the Theory of Computing, San Diego, May 1993
  (M. Karpinski, A. Sinclair)
- ICALP 93, Lund, Sweden, July 1993
  (M. Karpinski)
- Workshop on Randomness and Computation, Edinburgh, July 1993
  (M. Dyer, M. Jerrum, M. Karpinski, A. Lingas, C. J. H. McDiarmid, M. Santha, A. Sinclair, D. J. A. Welsh)

5 Other activities

An intensive exchange of research visits to participating sites and other leading research centers has took place as well as the exchange of postdoctoral students (in addition to the Workshops on "Randomized Algorithms" (Bonn, March '93), and on "Randomness and Computation" (Edinburgh, July '93)).

□