ESPRIT BR Working Group – 7097 (RAND)

Annual Progress Report

July 1, 1993 – June 30, 1994

Contents

1 Overview

The research within RAND in reporting period June 1, 1993 – July 30, 1994 was conducted again in all the main research areas of RAND:

(1) Design of Efficient Randomized Algorithms,

(2) Foundations of Randomized Complexity,

(3) Randomized Approximations Algorithms,

(4) Derandomizing Algorithms,

(5) Computational Learning Theory.

The research in Area (1) – (4) followed the lines described in Annual Progress Report 1992 / 1993.

Compared with the Annual Progress Report 1992 / 1993 the Research Area (5) Computational Learning Theory was extended considerably by the study of the VC Dimension of general quantified formulas, and applications in neural networks and commmputational geometry.

2 Research Papers (RAND)

(1) Angluin, D., Hellerstein, L. and Karpinski, M.:
Learning Read–Once Formulas with Queries,
in *Journal of ACM 40 (1993)*, pp. 185–210.

(2) Annan, J.:
A randomized approximation algorithm for counting the number of forests in dense graphs,
to appear in *Combinatorics, Probability and Computing*, 1994.

(3) Annan, J.:
Topics in computational complexity,
D. Phil. Thesis,
submitted in January 1994.

(4) Aronson, J., Dyer, M.E., Frieze, A.M. and Suen, S.:
On the greedy heuristic for matchings,
in *Proceedings of the 5^{th} Symposium on Discrete Algorithms*, pp. 141–149, ACM/SIAM Press, 1994.

(5) Boucheron, S.:
About maximum entropy methods in learning theory,
in *Proceedings on the Workshop on Algorithmic Complexity of Algebraic and Geometric Models, 1994*, (Beauquier, D., Slissenko, A. (Ed.)),
to appear in Lecture Notes in Computer Science, Springer–Verlag, 1994.

(6) Boucheron, S.:
About the Gibbs rule,
Communication at the Oxford RAND Workshop, March 1994.

(7) Boucheron, S.:
Sur les traces de l'apprentissage,
in *Proceedings of the 9^{th} RFIA 2 (1994)* (Gagalowicz, A., and Kayser, D. (Ed.))., pp. 1–13.

(8) Bshouty, N., Hancock, T., Hellerstein, L. and Karpinski, M.:
Read–Once Threshold Formulas Justifying Assignments and Generic Transformations,
Journal of Computational Complexity 4 (1994), pp. 37-61.

(9) Bshouty, N. Hancock, T., Hellerstein, L. and Karpinski, M.:
An Algorithm to Learn Read–Once Threshold Formulas, and some generic Transformations between Learning Models (Revised Version),
Technical Report No. TR–93–037, International Computer Science Institute, Berkeley, California, 1993.

(10) Chistov, A.L., Karpinski, M.:
Fast Interpolation Algorithms for Sparse Polynomials with Respect to the Size of Coefficients,
Research Report No. 85109–CS, Institut für Informatik, Universität Bonn, 1994.

(11) Cowling, P.:
Strong Total Chromatic Numbers of Complete Hypergraphs,
to appear in *Discrete Mathematics*, 1994.

(12) Cowling, P.:
Total Colouring of Hypergraphs,
Paper presented at the 8^{th} Midwest Conference on Combinatorics, Complexity and Computing, Wichita, USA, 1993,
to appear in *Journal of Combinatorial Mathematics and Combinatorial Computing*, 1994.

(13) Dyer, M.E., Frieze, A.M.:
Random walks, totally unimodular matrices and a randomized dual simplex method,
in *Mathematical Programming 64*, pp. 1–16, 1994.

(14) Dyer, M.E., Frieze, A.M. and Jerrum, M.R.:
Approximately counting hamilton cycles in dense graphs,
in *Proceedings of the 5^{th} Symposium on Discrete Algorithms*, pp. 336–343, ACM/SIAM Press, 1994.

(15) Dyer, M.E., Frieze, A.M., Kannan, R., Kapoor, A., Perkovic, L. and Vazirani, U.:

A mildly exponential time algorithm for approximating the number of solutions to a multidimensional knapsack problem,
in *Combinatorics, Probability and Computing 2 (1993)*, pp. 271–284.

(16) El Maftouhi, H.:
On the enumeration of random graded posets,
Communication at Oxford RAND Workshop, March 1994.

(17) Fernandez de la Vega, W.:
Average case analysis of the merging algorithm of Hwang and Lin,
Communication at Dagstuhl Workshop on "Average–case Analysis of Algorithms", July 1993.

(18) Fernandez de la Vega, W.:
Monte carlo algorithm for the approximation of the maximum consistent edge set in a tournament,
Communication at Oxford RAND Workshop, March 1994.

(19) Fernandez de la Vega, W., El Maftouhi, H.:
On random 2–sat,
Communication at Random graphs '93, 1993.

(20) Fernandez de la Vega, W., Kannan, S. and Santha, M.:
Two probabilistic results on merging,
in *SIAM Journal of Computing 22 (2)*, pp. 261–271, 1993.

(21) Fernandez de la Vega, W., Manoussakis, Y.:
Grids in random graphs,
in *Journal on Random structures and algorithms 5 (2)*, 1994.

(22) Fögel, A., Karpinski, M. and Kleine–Büning, H.:
Resolution for Quantified Boolean Formulas,
to appear in *Information and Computation 111 (2)*, 1994.

(23) Freivalds, R., Karpinski, M.:
Lower Space Bounds for Randomized Computation,
Research Report No. 85104–CS, Institut für Informatik, Universität Bonn, 1994,
Proceedings of the 21^{st} ICALP '94, Lecture Notes in Computer Science, Vol. 280, Springer-Verlag, 1994, pp. 580–592.

(24) Goldberg, P., Jerrum, M.:
Bounding the Vapnik Chervonenkis Dimension on Concept Classes Parametrized by Real Numbers, Proceedings of the 6^{th} ACM COLT, pp. 361–369.

(25) Grandvalet, Y., Canu, S. and Boucheron, S.:
Input perturbation in back propagation learning,
submitted.

(26) Grigoriev, D., Karpinski, M.:
Computing the Additive Complexity of Algebraic Circuits with Root Extracting,
submitted to *SIAM Journal of Computing (1993)*.

(27) Grigoriev, D., Karpinski, M.:
Lower Bounds on Complexity of Testing Membership to a Polygon for Algebraic and Randomized Decision Trees,
Technical Report No. TR–93–042, International Computer Science Institute, Berkeley, California, and Research Report No. 8599–CS, Institut für Informatik, Universität Bonn, 1994.

(28) Grigoriev, D., Karpinski, M. and Singer, M.:
Computational Complexity of Sparse Rational Interpolation,
in *SIAM Journal of Computing 23 (1994)*.

(29) Grigoriev, D., Karpinski, M. and Singer, M.:
Computational Complexity of Sparse Real Algebraic Function Interpolation,
in *Progress in Mathematics 109 (1993)*, Birkhäuser, pp. 91–104.

(30) Grigoriev, D., Karpinski, M. and Vorobjov, N.:
Lower Bounds on Testing Membership to Polyhedron by Algebraic Decision Trees,
Research Report No. 85103–CS, Institut für Informatik, Universität Bonn, 1993,
Proceedings of the 26th ACM STOC, 1994, pp. 635–644.

(31) Karpinski, M.:
Learning Read Once Formulas over Different Bases in Polynomial Time,
in Proceedings of the 3rd International Symposium on Artificial Intelligence, Wigry/Warsaw.

(32) Karpinski, M., Dahlhaus, E.:
An Efficient Parallel Algorithm for the Minimal Elimination Ordering (MEO) of an Arbitrary Graph,
in *Proceedings of the 30th IEEE FOCS*, pp. 454–459, 1989,
to appear in *Theoretical Computer Science*, 1994.

(33) Karpinski, M., Dahlhaus, E.:
On the sequential and Parallel Complexity of Matching in Chordal and Strongly Chordal Graphs,
Research Report No. 85107–CS, Institut für Informatik, Universität Bonn, 1994.

(34) Karpinski, M., Dahlhaus, E. and Hajnal, P.:
Optimal Parallel Algorithm for the Hamiltonian Cycle Problem on Dense Graphs,
Journal of Algorithms, 15 (1993), pp. 367–384.

(35) Karpinski, M., Grigoriev, D.Y., Singer, M.F.:
Interpolation of Sparse Rational Functions without Knowing Bounds on Exponents,
in *Proceedings of the 31st IEEE FOCS*, pp. 840–846, 1990, and in *SIAM Journal of Computing 23 (1)*, 1994, pp. 1–11.

(36) Karpinski, M., Macintyre, A.:
Polynomial Bounds for VC Dimension of Sigmoidal Neural Networks, Research Report No. 85116-CS, University of Bonn, 1994.

(37) Karpinski, M., Rytter, W.:
An Alphabet–Independent Optimal Parallel Search for Three Dimensional Patterns,
Proceedings of the 5th Symposium on Combinational Pattern Matching, 1994, *Lecture Notes in Computer Science*, Vol. 807 (1994), Springer-Verlag, pp. 125–135.

(38) Karpinski, M., Rytter, W.:
On a Sublinear Time Parallel Construction of Optimal Binary Search Trees,
Research Report No. 85102–CS, Institut für Informatik, Universität Bonn, 1994; in *Proceedings of MFCS '94*, *Lecture Notes in Computer Science*, Vol. 841 (1994), Springer-Verlag, pp. 453–461.

(39) Karpinski, M., Werther, T.:
VC Dimension and Uniforma Learnability of Sparse Polynomials and Rational Functions,
in *SIAM Journal of Computing 22 (1993)*, pp. 1276–1285.

(40) Karpinski, M., Werther, T.:
VC Dimension and Sampling Complexity of Learning Sparse Polynomials and Rational Functions,
to appear as a Chapter in the *Special Volume on Computational Learning Theory*, MIT Press, 1994.

(41) Karpinski, M., Zimmermann, W.:
Probabilistic Recurrence Relations for Parallel Divide–and–Conquer Algorithms,
Technical Report No. TR–91–067, International Computer Science Institute, Berkeley, California, 1991,
submitted to *Acta Informatica*, 1993.

(42) McDiarmid, C.J.H.:
A random recolouring method for graphs and hypergraphs,
in *Combinatorics, Probability and Computing 2 (1993)*, pp. 363–365.

(43) McDiarmid, C.J.H.:
Centering sequences with bounded differences,
submitted.

(44) McDiarmid, C.J.H.:
Hypergraph colouring and the Lovász Local Lemma,
submitted.

(45) McDiarmid, C.J.H.:
On first birth times for age–dependent branching processes,
submitted.

(46) McDiarmid, C.J.H., Edwards, K.:
New upper bounds for harmonious colourings,
in *Journal of Graph Theory* *18* *(1994)*, pp. 257–267.

(47) McDiarmid, C.J.H., Edwards, K.:
The Complexity of Harmonious Colouring for Trees,
to appear in *Discrete Applied Mathematics*, 1994.

(48) McDiarmid, C.J.H., Frieze, A. and Reed, B.:
On a conjecture of Bondy and Fan,
to appear in *Ars Combinatorica*, 1994.

(49) McDiarmid, C.J.H., Hayward, R.:
Large deviations for Quicksort,
submitted.

(50) McDiarmid, C.J.H., Hochberg, R. and Saks, M.:
On the bandwidth of triangulated cycles,
to appear in *Discrete Mathematics*, 1994.

(51) McDiarmid, C.J.H., Ramirez–Alfonsin, J.:
Sharing jugs of wine,
to appear in *Discrete Mathematics*, 1994.

(52) McDiarmid, C.J.H., Reed, B.:
Linear arboricity of random graphs,
submitted.

(53) McDiarmid, C.J.H., Reed, B., Schrijver, A. and Shepherd, B.:
Induced circuits in planar graphs,
in *Journal of Combinatorial Theory* *60* *(1994)*, pp. 169–176.

(54) McDiarmid, C.J.H., Sanchez–Arroyo, A.:
Total colouring regular bipartite graphs is NP–hard,
in *Discrete Mathematics* *24* *(1994)*, pp. 155-162.

(55) Santha, M., Tan, S.:
Verifying the determinant in parallel,
in *Proceedings of the* 5^{th} *International Symposium on Algorithms and Computation*,
to appear in Lecture Notes in Computer Science, Springer–Verlag, 1994.

(56) Santha, M., Vazirani, U.:
Parallel searching of multi–dimensional cubes,
in *Discrete Mathematics* <u>*114*</u>, pp. 425–443, 1993.

(57) Santha, M., Wilson, C.:
Polynomial size constant depth circuits with a limited number of negations,
in *SIAM Journal of Computing* <u>*22*</u> *(2)*, pp. 294–302, 1993.

(58) Thorup, M.:
Topics in Computation,
Awarded D.Phil., Oxford, January 1994.

(59) Welsh, D.J.A.:
Counting colourings and flows in random graphs,
to appear in *Colloq. Math. Soc. Janos Bolyai*, 1994.

(60) Welsh, D.J.A.:
Matroids: fundamental concepts,
to appear in *Handbook of Combinatorics*, 1994.

(61) Welsh, D.J.A.:
Random generation of polymer configurations,
to appear in *Probability, Statistics and Optimisation*, (Kelly, F.P. (Ed.)), 1994.

(62) Welsh, D.J.A.:
Randomized approximation schemes for Tutte-Gröthendieck invariants,
to appear in *Proceedings of the IMA Workshop on Probability and Algorithms University of Minnesota*, 1993.

(63) Welsh, D.J.A.:
Randomized approximations in the Tutte plane,
to appear in *Combinatorics, Probability and Complexity*, 1994.

(64) Welsh, D.J.A.:
The Random Cluster Process,
in *Discrete Mathematics* <u>*136*</u> *(1994)*, pp. 373–390.

(65) Welsh, D.J.A.:
The computational complexity of knot and matroid polynomials,
in *Discrete Mathematics* <u>*124*</u> *(1994)*, pp. 251-269.

(66) Welsh, D.J.A., Godsil, C. and Grätschel, M.:
Combinatorics in statistical physics,
to appear in *Handbook of Combinatorics*, 1994.

(67) Welsh, D.J.A., Lovász, L., Pyber, L. and Ziegler, G.M.:
Combinatorics in pure mathematics,
to appear in *Handbook of Combinatorics*, 1994.

3 Oxford Workshop on Randomized Algorithms (RAND), Oxford, March 22–25, 1994

The Workshop was organized by the ESPRIT BR Workshop Group on Randomized Algorithms (RAND), and the Mathematical Institute of the University of Oxford. As has been the case with the two previous RAND workshops it was principally concerned with those aspects of randomness of most interest in the design, analysis and implementation of probabilistic and randomised algorithms.

The workshop was held at Merton College. I am very grateful to Brenda Willoughby of the Mathematical Institute and the staff of Merton College for their help in organizing the meeting.

Dominic J.A. Welsh
April 1994

Abstracts of Talks

- **Stéphane Boucheron (LRI/Orsay):**
  About the Gibbs rule

  In learning theory, the use of the "Gibbs rule" has been promoted by researchers from statistical mechanics, as a general learning method to solve supervised learning problems. Here, we investigate the large sample size behaviour of this rule without using the implicit availability of a functional strong law of large numbers (the so-called self-averaging property). It is shown that for any reasonable temperature turning scheme (up to linear increase with sample size), the free-energy rate is a reversed submartingale, and that it converges towards a point random variable. The same holds for the other thermodynamical quantities. In the high temperature setting, there is no overfitting, but the prior is never completely forgotten hence the learning is never completed. In the fixed temperature, if the limiting value of the free energy rate is the infimum of the energy in the class of functions concerned, then the sequence of random posteriors enjoys a large deviation property, and optimal learning occurs in the limit.

- **Peter J. Cameron (Queen Mary & Westfield College/London, UK):**
  Random countable structures of given age

  The connection between enumerating a set and choosing a random element of the set is well known. This talk describeshow attempting to define probability measures on infinite sets leads to an unsolved enumeration question.

Let M be a countable relational structure. The age of M is the class of all finite structures embeddable (as induced substructure) in M. We assume that there are only finitely many n-element structures in Age (M) (up to isomorphism) for each n. (This holds if the relational language is finite.) The problem is to define a random countable structure whose age is contained in that of M. For each n-element structure $A \in \text{Age}(M)$ (on the set $\{1, ..., n\}$), and any n distinct points $x_1, ..., x_n$, we consider the basic event $E(x_1, ..., x_n; A)$ that the map $i \mapsto x_i$ $(i = 1, ..., n)$ is an embedding, and assign to it a probability $P(A)$ depending only on A.

The natural choice is to take

$$P(A) = \lim_{N \to \infty} P_N(A) \tag{1}$$

where

$$P_N(A) = \frac{\#\text{ structures in Age}(M)\text{ on }\{1, ..., N\}\text{ inducing }A\text{ on }\{1, .., n\}}{\#\text{ structures in Age}(M)\text{ on }\{1, ..., n\}}.$$

Problem 1. Does the limit (1) always exist?

As a special case, if M is a graph and A an edge, this asks whether the average edge-density in labelled N-vertex subgraphs of M tends to a limit. If the limit exists, then the probability measure is defined.

Problem 2. Is there a structure M_0 so that the random structure M is almost surely isomorphic to M_0?

Such an M_0 exists in several cases, e.g. graphs (it is Rado's universal graph), bipartite graphs, total orders (it is $\mathbb{R}$). Since almost all triangle-free finite graphs are bipartite, the random countable triangle-free graph is almost surely bipartite.

- **Alain Denise (Bordeaux):**
  Rejection algorithms for the random generation of words and combinatorial structures

  Rejection algorithms are often used to generate uniformly at random, combinatorial structures, as words, trees, graphs, polyominoes etc. In this talk, we are interested in such methods to generate words. Indeed, by using efficient encoding algorithms, the generation of many combinatorial structures can be reduced to the generation of words of particular languages.

  We study an improved rejection algorithm, the so-called florentine algorithm, to generate words of various languages. This method, first used by Barcucci, Pinzani and Sprugnoli to draw Motzkin left factors at random (and then directed animals with an appropriate encoding due to Penaud), improves the time complexity of the "classical" rejection algorithm. In most cases, only lower and upper bounds can be given for the average complexity of the florentine algorithm. However, we introduce the family of "fg-languages", set of languages for which it can be computed exactly. Our proofs are based on some basic properties of maximal prefix codes.

- **Martin Dyer (University of Leeds):**
  Counting contingency tables

  The problem of counting contingency tables arises in statistical inference (Diaconis and Efron). We show that in general this problem is $\#P$-complete. We show that a fully polynomial randomized approximation scheme (fpras) exists in a restricted case: that, for a problem with m rows and n columns, all row totals are at least n^2m and all column totals at least m^2n. This is achieved by an almost uniform generation algorithm, which is of interest in its own right for statistical applications. The algorithm is a variant of random walk algorithms suggested by Diaconis for this problem, but for which little theoretical support previously existed. The general case remains open.

- **Artur Ekert (Merton College/Oxford):**
  Brief introduction to quantum computation

  As computers become faster they must become smaller, because of the finiteness of the speed of light. On an atomic scale physical carriers of information have to obey the laws of quantum mechanics and quantum effects must be taken into account in designing microelectronic circuits. Some quantum phenomena, in particular quantum interference, allow fundametally new forms of computation and as a result a new mathematical model of computation is necessary to analyse the power of quantum computation.

  Quantum Turing Machines introduced by Deutsch and formalized by Bernstein and Vazirani are probabilistic models of computation, similar to the Probabilistic Turing Machines but with transition rules specified by the probability amplitudes rather than probabilities. In my talk Quantum Turing Machines are defined and compared with Probabilitic Turing Machines. An alternative model of quantum computation namely quantum Boolean circuits are mentioned in connection with practical realisation of quantum computers. Universal quantum logic gates are defined and their implementation based on optically controlled quantum dots in semiconductors is briefly explained.

- **Hakim El Maftouhi (Universite Paris–Sud):**
  Enumeration of graded posets with fixed width

  We give a procedure for computing the number $N(\omega, r)$ of distinct graded partial orders of width ω and r. For any fixed ω the procedure requires a computation time linear in r.

- **Ulrich Faigle, R. Garbe & Walter Kern (University of Twente/ Netherlands**

  Randomized online algorithms for maximizing busy time

  We consider a simple one-machine scheduling problem given by a set of tasks, i.e., intervals. The problem is to find a (probabilistic) online algorithm with reasonable worst case performance ratio. We answer an open problem of Lipton and Tompkins concerning the best possible ratio that can be achieved. Furthermore, we extend their results to an m-machine analogue. Finally a variant of the problem is analyzed, in which the algorithm is allowed to remove the currently processed job.

- **W. Fernandez de la Vega (Laboratoire de Recherche en Informatique, CNRS, UA 410/Université de Paris-Sud, Bât 490, 91405 Orsay Cedex/France):**

  A Monte–Carlo approximation for the maximum size of a consistent set of arcs in a tournament

  A set of arcs in a tournament is said to be consistent if it doesn't contain any circuit. For any $\epsilon > 0$ and $0 < p < 1$, we give a randomized algorithm which runs in polynomial time and which, when applied to any given tournament T, outputs a number $A(T)$ which satisfies with probability $\geq p$ the inequalities $(1-\epsilon)CONS(T) \leq A(T) \leq CONS(T)$ where $CONS(T)$ is the maximum size of a consistent set of arcs in T.

- **David A. Grable (Forschungsinstitut für Diskrete Mathematik/ Universitat Bonn):**

  Asymptotic enumeration of packings in hypergraphs

  I discuss a recent result which states that for fixed k, if $\mathcal{H}$ is a collection of k-uniform hypergraphs such that for $H \in \mathcal{H}$, $\mathrm{mindeg}(H) = (1-o(1))\mathrm{maxdeg}(H)$ and $\mathrm{maxcodeg}(H) = o(\mathrm{maxdeg}(H))$ then H contains

  $$\exp\left\{(1+o(1))\frac{|V(H)|}{k}\ \ln\ \mathrm{maxdeg}\ (H)\right\}$$

  packings (collections of disjoint edges). The proof is based on the analysis of a randomized hypergraph packing algorithm.

  One application of this result is that there exist

  $$\exp\left\{(1+o(1))\frac{k-t}{k_{(t)}}n^t \ln\ n\right\}$$

  partial t-designs with blocks of size k on n points.

- **Mark Jerrum (Department of Computer Science/University of Edinburgh):**

  A very simple algorithm for estimating the number of k-colourings in a low-degree graph

A fully polynomial randomised approximation scheme (fpras) is presented for estimating the number of (vertex) k-colourings of a graph G of maximum degree Δ, when $k \geq 2\Delta+1$. The approximation scheme is based on the simplest possible Markov chain on k-colourings of G: select a vertex V u.a.r. and a colour c u.a.r. and attempt to recolour vertex v with colour c. This Markov chain is ergodic for $k \geq \Delta + 2$ and its stationary distribution is uniform.

A coupling argument is used to show that the Markov chain is "rapidly mixing" when $k \geq 2\Delta+1$, and hence provides an efficient sampling procedure for k-colourings of G. An fpras for k-colourings follows via a standard reduction from approximate counting to sampling. The existence of an fpras for k-colourings when k is in the range $\Delta \leq k \leq 2\Delta$ is open; no fpras can exist when $k < \Delta$ (unless $RP = NP$) since the related decision problem is NP-complete.

- **Richard Jozsa (School of Mathematics and Statistics/University of Plymouth):**
  Quantum complexity theory – an overview

  The question of whether quantum computing machines are more efficient than their classical counterparts, remains open. We describe recent work of various people having a bearing on this question. Our model of quantum computation is the Deutsch/Bernstein-Vazirani QTM which is used to define quantum analogues of the standard complexity classes. A QTM may be thought of as a branching tree of complex "probability amplitudes" or alternatively as a PTM of the usual kind, except that probabilities are allowed to become negative (Feynman). QTM's are seen to exhibit non-classical modes of computation e.g. "computation by quantum parallelism". Various relativised separation results are described. Oracles may be constructed which separate QP from P (Deutsch, Jozsa) and $QBPP$ from BPP (D. Simon).

- **Marek Karpinski (University of Bonn):**
  Lower bounds for randomized computation trees

  We introduce a new method for proving lower bounds for algebraic computation trees. We prove, for the first time, that the minimum depth for any randomised computation tree for the problem of testing membership to a polygon with N nodes is $\Omega(\log N)$ (the method also yields the first $\Omega(\log N)$ lower bound for the deterministic computation trees). Moreover, we prove that the corresponding lower bound for the algebraic exp-log computation trees is $\Omega(\sqrt{\log N})$.
  (Joint work with D. Grigoriev)

- **Christos Levcopoulos (University of Lund):**
  Tail estimates for QUICKSORT and related problems

Let $P(c)$ be the probability that QUICKSORT performs at least $c - n \log n$ comparisons. On the other hand, let $P'(c')$ be the probability that the selection algorithm FIND performs more than $c'n$ comparisons. We try to estimate $P(c)$ and $P'(c')$, for growing c and c'.

For large c and c' we have

$$P(c) = \left(\frac{1}{n}\right)^{\Theta(c - \log\log n)}$$

and

$$P'(c') = \left(\frac{1}{2}\right)^{\Theta(c' \log c')}.$$

Independently, the function $P(c)$ had been investigated by Colin McDiarmid and others.

- **Andrej Lingas (jointly with A. Dessmark and O. Garrido) (University of Lund):**

  Partial results on the parallel complexity of the degree sequence problem

  The degree sequence problem (DSP for short) is for a sequence of natural numbers $d_1, d_2, ..., d_n$ to construct if possible a simple graph on n nodes such that the degree of the i-th node is d_i, $i = 1, ..., n$. We observe DSP to be in the randomised NC class by reduction to maximum matching (via maximum f-matching). On the other hand, we observe that the decision version of DSP admits a logarithmic-time work-optimal NC algorithm by Erdös-Gallai's inequalities. We provide an NC approximation algorithm for the construction version of DSP. Our main result is an NC algorithm for constructing if possible a graph satisfying the degree equality constraints $d_1, d_2, ..., d_n$ in case $d_i \leq \sqrt{\sum_{j=1}^{n} dj}/5$ for $i = 1, ..., n$.

- **Colin McDiarmid (Department of Statistics/University of Oxford):**

  On 2-colouring a 3-colourable graph to avoid monochromatic triangles

  Recently Papadimitriou has proposed a randomised method for solving the 2- satisfiability problem; and the author has proposed a randomised recolouring method which, given a 3-colourable graph, finds a 2-colouring of the vertices so that no triangle is monochromatic. Both methods involve finding a 'bad' configuration (unsatisfied clause, monochromatic triangle) and randomly changing one of the bits involved.

  In this talk we see how these problems fit naturally in a more general geometric context; and how the two similar random solution methods are both special cases of a simple 'bit-flipping' method for the more general problem, for which similar results hold. Further, we consider deterministic methods to handle such problems, and in particular show that we can solve the above 'triangle problem' in polynomial time.

- **Milena Mihail (Bellcore and Athens):**
  On the random walk method for protocol testing

  For large protocols traditional testing techniques become prohibitively complex, and testing by random simulation is the only general engineering alternative; implicit in such random simulations is a random walk. Relevant to the effectiveness of the random walk method for testing are mixing (and cover time) arguments; we discuss how such arguments apply to various families of protocols.

- **Angelika Steger (University of Bonn):**
  Probabilistic checking of proofs

  In 1992 Arora, Lund, Motwani, Sudan and Szegedy proved a new characterization of the class NP in terms of probabilistically checkable proofs. Not only is this new result, which can be formally phrased as $NP = PCP(\log n, 1)$, interesting and surprising for its own sake — it also has far-reaching consequencdes for the approximability of combinatorial optimization problems. The aim of this talk is to explain this result and to survey its consequences and recently obtained generalizations.

- **Miklos Santha and Sovanna Tan (Université Paris–Sud):**
  Verifying the determinant in parallel

  In this paper we investigate both in the Boolean arithmetic circuit and the Boolean circuit model the complexity of the verification of problems whose computation is equivalent to the determinant. We observe that for a few problems there exist an easy (NC^1) verification algorithm. To characterize the harder ones, we define under two different reductions the class of problems which are reducible to the verification of the determinant and establish a list of complete problems in these classes. In particular we prove that computing the rank is equivalent under AC^0 reduction to verifying the determinant. We show in the Boolean case that none of the complete problems can be recognized in NC^1 unless $L = NL$. On the other hand we show that even for problems which are hard to verify there exists an NC^1 checker and that they can be extended into problems whose verification is easy.

- **Friedhelm Meyer auf der Heide, Christian Scheideler and Volker Stemann (Heinz Nixdorf Institute/University of Paderborn):**
  Fast simple dictionaries and shared memory simulations on Distributed Memory Machines, upper and lower bounds

  Assume that a set U of memory locations is distributed among n memory modules, using some number a of hash functions $h_n, ..., h_a$, randomly and independently drawn from a high performance universal class of hash-functions. Thus each memory location has a copies: Consider the task of accessing b out of the a copies for each keys $x_1, ..., x_{\varepsilon n} \in U$, $b < a$ and

$0 < \varepsilon \leq 1$. We present and analyse a process executing the above task on distributed memory machines (DMMs) with n processors. Efficient implementations are presented, implying

- a simulation of an n-processor $PRTM$ on an n-processor optical crossbar DMM with delay $O(\log\log n)$.
- a simulation as above on an arbitrary DMM with delay

  $$O\left(\frac{\log\log n}{\log\log\log n}\right),$$

  the fastest known $PRTM$ simulation,
- a static dictionary with parallel access time

  $$O\left(\log^4 n + \frac{\log\log n}{\log a}\right),$$

  if **a** hashfunctions are used. In particular, an access line of $O(\log^4 n)$ can be reached if $(\log n)^{1/\log^4 n}$ hashfunctions are used.

We further prove a lower bound for executing the above process, showing that our implementations are optimal.

- **Jacobo Toran (Barcelona):**
  Lowness and counting

  Informally, a set A is low for a complexity class C if A does not help C when used as oracle, that is, if $C^A = C$. We give a survey of known results in the area of counting complexity classes showing that these results can be explained in a uniform way using the concept of lowness. In particular we show that the complexity classes UP and BPP and the Graph Isomorphism and Automorphism problems are low for PP, and that the classes $\oplus P$, NP and PH are low for P^{PP}, thus giving with this last result an alternative proof of Toda's theorem.

- **R. Verbeek (Hagen):**
  Some results on the separation of randomized time

  While it is easy to separate probabilistic complexity classes (with unbounded error), the separation of Monte Carlo (bounded error) complexity classes with different (constructible) bounds is one of the most challenging problems in randomized complexity theory. For example it is not known whether or not $BPP = BPTIME(n)$. We have a few observations that may enlighten the difficulties of the problem.

  (1) If $BPTIME(n) = BPP$, then there is a *weak translation*: there is some recursive h s.t. for any poly-time Monte Carlo machine, $h(i)$ is a probabilistic linear time machine, which computes ϕ_i with bounded error for almost all inputs. (ϕ_i denotes the function computed by the i-th probabilistic Turing machine with 0-1 valued output.)

(2) A *strong translation* between BPP and $BPTIME(n)$ is not possible. There is no recursive h with the following properties: if i is a poly-time Monte-Carlo machine, then $h(i)$ computes ϕ_i with bounded error for all inputs.

(3) We define partial Monte-Carlo computable functions by:

$$\tilde{\phi}_i(x) := \begin{cases} \phi_i(x) \text{ if } err_i(x) < \frac{1}{4} \text{ (bounded error on input } x) \\ \text{undefined otherwise} \end{cases}$$

and $\widetilde{BPTIME}(f)$ as the set of all functions $\tilde{\phi}_i$ computable by machines with $f(n)$-bounded running time. Since the domains of functions in $\widetilde{BPTIME}(f)$ are just the sets in Pr Time (f), obviously $\widetilde{BPTIME}(u) \neq \widetilde{BPP}$. Less obvious is the following theorem:

There is a 0-1-valued partial function $l \in \widetilde{BPP}$, s.t. for any $g \in \widetilde{BPTIME}$ with infinite domain, f and g differ on dom$(f) \wedge$ dom(g).

(4) For almost all oracles A, $BPTIME^A(u) \neq BPP^A$. Fortnow and Sipser claimed $BPTIME^A(n) = BPP^A$ even $ZPTIME^A(n) = BPP^A$) for some oracle A ($STOC$ '89). Unfortunately the proof contains several gaps and up to now the authors were not able to fill them. We have a new oracle construction and can in fact prove that $BPTIME^A(n) = BPP^A$ for some (recursive) oracle A. Thus it is not possible to show $BPTIME(n) \neq BPP$ by any relativizing technique.

There are several problems (not only for randomized complexity classes) where a separation fails for similar reasons as in the BP-case, e.g.

$$ZPTIME(n) \neq ZPP,$$

$$NTIME(n) \cap \text{co} - NTIME(n) \neq NP \wedge \text{co} - NP.$$

It is open, whether or not these problems are also oracle dependent.

- **Paul Vitanyi (Amsterdam):**
Introduction to Kolmogorov complexity and its applications

Kolmogorov complexity is the theory dealing with the quantity of information in individual objects. It is also known as 'algorithmic information', 'algorithmic entropy', 'Kolmogorov-Chaitin complexity', 'descriptional complexity', 'shortest program length', 'algorithmic randomness', and others. It is an asolute and objective notion by Church's thesis and the ability of universal machines to simulate one another. Applications include randomness of individual finite objects or infinite sequences, Martin-Loef tests for randomness, Gödel's incompleteness result, information theory of individual objects, universal probability, general inductive reasoning, inductive inference, prediction, mistake bounds, computational learning theory, inference in statistics, the incompressibility method, combinatorics, time and space complexity of computations, average case analysis of algorithms such as HEAPSORT, language recognition, string matching, formal language and automata theory, parallel computation, Turing machine complexity, lower bound proof techniques, probability theory, structural complexity theory, oracles, logical depth, universal optimal search, physics and computation, dissipationless reversible computing, information distance and picture similarity, thermodynamics of computing, statistical thermodynamics and Boltzmann entropy. We present the basics of the theory and a range of applications. This talk is based on the (text)book by Ming Li and Paul Vitanyi, An Introduction to Kolmogorov Complexity and Its Applications, Springer-Verlag, 1993.

4 ICMS Workshop "Randomness and Computation", Edinburgh, July 26–30, 1993

A workshop on *Randomness and Computation* took place at Edinburgh University during the week 26th – 30th July, forming part of a wider ICMS[1] Research Programme that had included a workshop on *Algebraic Graph Theory* two weeks earlier. The scientific committee for the workshop was Persi Diaconis (Harvard), Mark Jerrum (Edinburgh) and Alistair Sinclair (Edinburgh). Seven SERC Visiting Fellows – David Aldous (Berkeley), Noga Alon (Tel Aviv), Persi Diaconis, Martin Dyer (Leeds), Peter Sarnak (Princeton), Roberto Schonmann (UCLA), and Avi Wigderson (Jerusalem) – provided a core of one–hour survey talks, which were complemented by numerous shorter contributed talks from some of the 50 or so other participants.

The scientific committee were keen to bring together researchers from different disciplines, who were nevertheless working on what seemed to be related problems. The interdisciplinary nature of the workshop was reflected in the participant list, which featured statisticians, combinatorialists, theoretical computer scientists, probabilists, and physicists (well, one physicist at least). By the middle of the workshop, any initial apprehension the organisers may have felt over the participants' ability to find a common language had evaporated, as it became apparent that the workshop was achieving its key objective. Credit for the success of the meeting goes to the various speakers for their contributions, which were almost without exception of a high standard, and to Frank Donald of the ICMS for ensuring the smooth running of the whole enterprise.

The research programme was supported by the UK Science and Engineering Research Council, London Mathematical Society, and by the Esprit "RAND" Working Group.

Persi Diaconis, Mark Jerrum, and Alistair Sinclair
August 17, 1993

[1]International Centre for Mathematical Sciences, Edinburgh

Abstracts of Talks

- **David Aldous (UC Berkeley):**
  Useful results from a first-year graduate probability course

  Although much of mathematical probability may be irrelevant to the probability/ algorithms area, there are still a lot of standard techniques that are useful. I shall give simple applications of the martingale optional sampling theorem, martingale maximal inequalities, and the subadditive ergodic theorem.

- **Noga Alon (Tel Aviv University):**
  Derandomization via small sample spaces

  In many randomized algorithms a certain amount of limited independence between the required random choices suffices. Some of these algorithms can be converted into efficient deterministic ones by using d-wise independent random variables over polynomial size sample spaces. Here we survey briefly the construction of such spaces and their applications, focusing on the related notion of k-wise ϵ-biased random variables defined over small sample spaces and some of its recent applications.

- **James Annan (University of Oxford):**
  A fully polynomial randomised approximation scheme for the number of forests in a dense graph

  The problem of counting the number of forests in a graph is considered. Attention is restricted to the class of dense graphs, in which each vertex has degree at least αn, where α is a fixed positive constant and n is the number of vertices of the graph. A polynomial time randomised algorithm is presented for uniformly generating the forests in a dense graph. Using this, and an idea of Jerrum, Valiant and Vazirani, a fully polynomial randomised approximation scheme (fpras) for counting the number of forests in a dense graph is created.

- **Alain Denise (LaBRI, Bordeaux I):**
  Rejection algorithms for the generation of words

  Barcucci, Pinzani and Sprugnoli designed an improvement of a classical rejection method in order to generate uniformly at random Motzkin left factors and underdiagonal walks in linear average time and space. We present a generalization of this method to other languages, and we study its complexity. Generally, only lower and upper bounds can be given for it. We define the "fg-languages", a class of languages for which the complexity can be computed exactly. We apply the method to some particular fg–languages.

- **Persi Diaconis (Harvard University):**
  From statistics to toric ideals and back

  We construct Markov chain algorithms for sampling from discrete exponential families conditional on a sufficient statistic. Examples include generating tables with fixed row and column sums, and higher dimensional analogs. The algorithms involve finding bases for associated polynomial ideals, and hence an excursion into computational algebraic geometry.

- **Martin Dyer (University of Leeds):**
  Estimating the volume of convex bodies

  Determining the volume of convex bodies is known to be very hard. There is an oracle model for the problem within which even approximation can be shown to be impossible in polynomial time by any *deterministic* algorithm. By contrast, there is a *randomized* algorithm which permits approximation to arbirary relative error in polynomial time (a fully polynomial randomized approximation scheme). We outline this algorithm (due to Dyer, Frieze and Kannan (1989)) and subsequent improvements due to Applegate and Kannan, Lovász and Simonovits and others.

- **Jim Fill (Johns Hopkins University):**
  Markov chains and self-organizing data structures

  Self–organizing data structures, which dynamically maintain a file of records in easily retrievable order while using up little memory space, have been investigated by probabilists and computer scientists for more than 25 years. Such self-organizing systems have been applied to problems in very large-scale integration (VLSI) circuit simulation, data compression and communications networks. I will discuss the application of techniques for analyzing Markov chains to the study of self-organizing lists and other data structures. This talk will focus on the *move-to-front (MTF) rule* for linear search lists (otherwise known as the *Tsetlin library*), and the *move-to-root (MTR) rule* for binary search trees. A key result is that the MTF lumps to the MTR in a natural way.

- **David Gillman (MIT):**
  A Chernoff bound for random walks on expander graphs

  A finite trajectory of the random walk on a weighted graph G is considered; the sample average of visits to a set of vertices A is shown to converge to the stationary probability $\pi(A)$ with error probability exponentially small in the length of the random walk and the square of the size of the deviation from $\pi(A)$. The exponential bound is in terms of the expansion of G and improves previous results of Aldous, Lovász and Simonovits, and Ajtai, Komlós, and Szemerédi. The method of taking the sample average from a single trajectory is shown to be a more efficient estimator of $\pi(A)$ than the standard method of generating independent sample points from several trajectories. This more efficient sampling method is used, together with other statistical innovations, to improve the running times of the algorithms of Jerrum and Sinclair for approximating the number of perfect matchings in a wide class of graphs and for approximating the value of the partition function of a ferromagnetic Ising system. A fast estimate of the entropy of a random walk on an unweighted graph, considered as an information source, is also given.

- **Leslie Goldberg (Sandia National Laboratories):**
  Randomized algorithms for communication in optical networks

  We consider the problem of interprocessor communication on a *Completely Connected Optical Communication Parallel Computer* (OCPC). The particular problem we study is that of realizing an *h-relation*. In this problem, each processor has at most h messages to send and at most h messages to receive. It is clear that any 1-relation can be realized in one communication step on an OCPC. However, the best known p-processor OCPC algorithm for realizing an arbitrary h-relation for $h > 1$ requires $\Theta(h + \log p)$ expected communication steps. (This algorithm is due to Valiant and is based on earlier work of Anderson and Miller.) Valiant's algorithm is optimal only for $h = \Omega(\log p)$ and it is an open question of Geréb-Graus and Tsantilas whether there is a faster algorithm for $h = \wr(\log p)$. In this paper we answer this question in the affirmative by presenting a $\Theta(h + \log\log p)$ communication step algorithm that realizes an arbitrary h-relation on a p-processor OCPC. We show that if $h \leq \log p$ then the failure probability can be made as small as $p^{-\alpha}$ for any positive constant α. (Joint work with Mark Jerrum, Tom Leighton and Satish Rao)

- **Marek Karpinski (University of Bonn):**
  Derandomization and the explicit simulation of small depth threshold circuits

  Using a *derandomization* technique, we prove that a single threshold gate can be simulated by an *explicit* polynomial size depth 2 majority circuit. In general we show that a depth d threshold circuit can be simulated uniformly by a majority circuit of depth $d + 1$. Our construction answers two open problems of Goldmann, Håstad and Razborov (1992): we give the first explicit construction where they use a randomized existence argument, and we show that such a simulation is possible even if the depth grows with the number of variables n. Our results entail the first explicit constructions for optimal depth, polynomial size majority circuits for a number of basic functions, including *powering* (depth 3), *integer multiplication* (depth 3), and *integer division* (depth 3).
  (Joint work with M. Goldmann)

- **Andrzej Lingas (Lund University):**
  Maximum cardinality f-matching is in RNC

  We present an NC^1 reduction of maximum (cardinality) f-matching to maximum (cardinality) matching, which yields a randomized NC algorithm for constructing a maximum f-matching. As a result, we also obtain a randomized NC solution to the problem of constructing a graph satisfying a sequence of equality degree constraints.

- **Francesco Maffioli (Politecnico di Milano):**
  Polynomial identities and matroid parity: a survey

  Recent results are surveyed exploiting the possibility of testing multivariate polynomial identities in random polynomial time as a tool for solving some NP-hard combinatorial programming problems. Algorithms running in pseudo-polynomial time have been obtained for finding a base of given value in a represented matroid subject to parity conditions with elements weighted in the integers, or proving that such a base does not exist. In order to obtain the best possible worst-case complexity, the algorithms use fast arithmetic working over a suitable randomly chosen finite field. Special cases include matroid intersection of exact value and exact cost flows in acyclic graphs. The algorithms considered allow one also to compute in pseudo-polynomial time the entire set of feasible values of solutions (viz. the "image") of an instance of such problems. The parallel complexity of these problems has also been addressed and the basic problem of constructing an exact parity base is shown to belong to arithmetic RNC^2, under the similarity assumption. Extensions and open problems are also discussed.

- **Fabio Martinelli (La Sapienza, Rome):**
  Approach to equilibrium of the Gibbs sampler in the one-phase region

  Some results obtained in collaboration with E. Olivieri on rapid convergence to equilibrium of the Gibbs sampler for a discrete "spin" Gibbs measure of the cubic lattice, under certain finite volume conditions, will be illustrated. Our conditions on the Gibbs measure imply a suitable "weak dependence" of the measure in finite volume on the boundary conditions. Our results are optimal in the sense that, for example, they show for the first time fast convergence of the dynamics for any temperature above the critical one for the d-dimensional Ising model with or without an external field. In the general case, not necessarily the usual Ising model, using renormalization group ideas, hypercontractivity of the Markov semigroup of the Gibbs sampler is proved under a suitable condition on the Gibbs measure via a Logarithmic Sobolev Inequality. It will also be illustrated by means of concrete examples how the geometric shape of the volume in which the Gibbs sampler is considered can dramatically slow down the convergence to equilibrium.

- **Colin McDiarmid (University of Oxford):**
  A random recolouring method for graphs and hypergraphs

  We discuss a simple randomised algorithm that seeks a weak 2-colouring of a hypergraph H; that is, it tries to 2-colour the points of H so that no edge is monochromatic. If H has a particular well-behaved form of such a colouring, then the method is successful within an expected number of iterations $\mathcal{O}(n^3)$, where n is the number of points in H. In particular, when applied to a graph G with n vertices and chromatic number 3, the method yields a 2-colouring of the vertices such that no triangle is monochromatic, in expected time $\mathcal{O}(n^4)$. (Following thoughts stimulated at the meeting, I have now found a deterministic method for solving such problems.)

- **Milan Merkle (University of Belgrade):**
  Systems of stochastic differential equations on duals of nuclear spaces

  We consider a self-adjoint differential operator L defined on a dense linear subspace of a Hilbert space $H^{\otimes N}$, which is the Nth direct power of a given Hilbert space H. Then we find a suitable nuclear space $\Phi \subset H^{\otimes N}$ so that the system of stochastic differential equations

  $$d\xi_t = -L'\xi_t dt + dW_t$$

  has a solution on $\Phi' \supset H^{\otimes N}$, where W_t is a Wiener process on Φ'. Further we show that a class of equations of the above form can be solved by diagonalization, and we prove a propagation of chaos result. As an application, we discuss a model that describes interaction between a large number of neurons.

- **Noam Nisan (Hebrew University, Jerusalem):**
  More deterministic simulation in Logspace

  We show that any randomized (S) algorithm which uses only poly(S) random bits can be simulated deterministically in (S), for $S(n) \geq \log n$. Of independent interest is our main technical tool: a procedure which extracts randomness from a defective random source using a small additional number of truly random bits. (Joint work with David Zuckerman)

- **Rafail Ostrovsky (UC Berkeley and ICSI, Berkeley):**
  Interactive hashing for cryptographic protocols

  In this talk we describe the technique of *interactive hashing*: given any one-way permutation f, two players can efficiently choose $\{y_0 y_1\}$ such that one player can compute $f^{-1}(y_b)$, $b \in \{0,1\}$, and provably cannot find $f^{-1}(y_{1-b})$, while b is hidden information-theoretically from the other player. We stress that our scheme is *efficient*: both players execute only polynomial-time programs during the protocol. We exhibit several applications of this technique.

- **Ljiljana Petrović (University of Kragujevac):**
Causality and Markovian representations of a family of Hilbert spaces

  The basic idea in this paper is to relate some concepts of causality to the stochastic realization problem. More precisely, we consider the following problem (which follows directly from the realization problem): how to find a minimal (respectively, maximal) Markovian flow of information G (understood as a family of Hilbert spaces) that contains (respectively, is contained in) a given flow of information E and is such that each of these two flows of information gives the same information about the flow E.

- **Dana Randall (UC Berkeley):**
Testable algorithms for self-avoiding walks

  We present a polynomial time Monte Carlo algorithm for almost uniformly generating and approximately counting self-avoiding walks in rectangular lattices $\mathbb{Z}^d$. These are classical problems that arise, for example, in the study of long polymer chains. While there are many Monte Carlo algorithms used to solve these problems in practice, these are heuristic and their correctness relies on unproven conjectures. In contrast, our algorithm relies on a single, widely-believed conjecture that is less restrictive than preceding assumptions, and, more importantly, is one which the algorithm itself can test. Thus our algorithm is *reliable*, in the sense that it either outputs answers that are guaranteed, with high probability, to be correct, or finds a counterexample to the conjecture.
  (Joint work with Alistair Sinclair)

- **Lars Rasmussen (University of Edinburgh):**
Approximating the permanent: a simple approach

  The problem of deciding whether a bipartite graph contains a perfect matching is well known to be in P. In contrast, the corresponding counting problem, that of computing the permanent of a square (0-1) matrix, is known to be #P-complete and hence apparently intractable. For this reason, the permanent plays the role of a benchmark problem in complexity theory. In this talk, we present a very simple randomised approximation algorithm for the permanent. As the main result, we prove that our algorithm, even though its worst case behaviour is provably very bad, runs in time polynomial in the size of the input matrix for almost all matrices. We also present various improvements to the basic technique, and some preliminary results regarding their efficiency. We will also demonstrate how the simplicity of our approach allows our algorithm for the permanent to be adapted to approximate the number of Hamilton cycles in almost every directed graph.

- **Jeffrey Rosenthal (Minnesota):**
Convergence of independent particle systems

We consider a system of particles moving independently on a countable state space, according to a general (non-space-homogeneous) Markov process. Under mild conditions, the number of particles at each site will converge to a product of independent Poisson distributions; this corresponds to settling to an ideal gas. We derive sharp bounds on the rate of this convergence. In particular, we prove that the variation distance to stationarity decreases proportionally to the sum of squares of the probabilities of each particle being at a given site. Our methods include a simple use of the Chen-Stein lemma about Poisson convergence.

- **Laurent Saloff-Coste (Paris VI):**
Time to equilibrium of exclusion processes

This talk reports on joint work with P. Diaconis which will appear in *Annals of Applied Probability*, 1993. Let (X, E) be a finite regular graph. Consider the exclusion process in which m particles hop around on (X, E). We compare this process with the Bernoulli-Laplace process, whose eigenvalues are known. The comparison yields upper and lower bounds on the spectral gap λ of the exclusion process in terms of the geometry of (X, E). For instance, if (X, E) is the circle graph with $2n$ vertices, and if there are $m = n$ particles, we get $\frac{1}{2n^3} \leq \lambda \leq \frac{\pi^2}{32n^3}$. This technique works for many other graphs. In this example, one can use logarithmic Sobolev techniques to show that equilibrium is reached after $\mathcal{O}(n^3(\log n)^2)$ steps, whereas n^3 steps are necessary. These results improve on previous work by Jim Fill. A recent paper of J. Quastel (*Comm. Pure. Appl. Math*, 1992) contains closely related results.

- **Peter Sarnak (Princeton University):**
Quantum arithmetic chaos

The eigenvalue distribution (in particular the level spacing) of a random matrix serves as a model for the level spacing of the Laplace eigenvalues of a classically chaotic geodesic flow. Similarly, a random wave model serves to describe the behavior of the eigenfunctions (as λ tends to infinity). First we report on numerical investigations of the above "conjectures." Second, in the case that the manifold is constructed arithmetically, we bring in techniques from number theory to investigate these fine spectral questions. It is shown (somewhat surprisingly) that the spectrum follows a Poisson-like level spacing even though the classical dynamics is chaotic. On the other hand, the eigenfuntions are shown to behave like random waves—a phenomenon which is shown to be closely tied to the classical Lindelöf Hypothesis for the Riemann Zeta function.

- **Roberto Schonmann (UCLA):**
Stochastic evolution of Ising models

In these two talks I plan to explain how a technique developed in Computer Science to estimate the rate of convergence of Monte Carlo simulations of combinatorial structures turned out to be essential in the solution of a problem in non-equilibrium statistical mechanics. The problem concerns the speed of relaxation of statistical mechanical systems in the proximity of the phase-transition region, and is related to the problem of understanding the metastable behavior of systems in such regions. For instance, it is well known that a ferromagnetic material which is in equilibrium under a negative external magnetic field relaxes to equilibrium very slowly after the magnetic field is switched to a small positive value. A detailed mathematical analysis of such a phenomenon can only be performed on simplified models. It is widely accepted that an appropriate model for this and many other purposes is a *stochastic Ising model*, i.e., a Markov process which endows the traditional Ising model with a particular stochastic dynamics. On each vertex of an infinite lattice $\mathbb{Z}^d$, there is a variable (called a *spin*) which takes the value -1 or $+1$. The system evolves in continuous time as a Markov process which is time-reversible and has as invariant measures the classical Gibbs measures of statistical mechanics. Provided the "temperature" parameter appearing in the definition of the model is small enough, a phase transition takes place when the "external field" parameter, h, changes sign. (This corresponds to the majority of spin values changing from $+1$ to -1.) The question then arises of how the system relaxes to equilibrium when h is small (positive say), and the system is initially in the configuration with all spins -1. In equilibrium the spins have to be mostly $+1$, with the -1-spins forming finite clusters in a background of $+1$-spins. Simulations have shown that the relaxation mechanism is driven by the behavior of the clusters (or *droplets*) of $+1$-spins which form initially in the sea of -1-spins. While small droplets tend to shrink and disappear, large ones tend to grow and are responsible for the relaxation. This phenomenon has long been understood on non-rigorous heuristic grounds, and can be used to predict for instance the order of magnitude, as $h \searrow 0$, of the relaxation time for the process. The prediction is that the relaxation time grows as $\exp(C/h^{d-1})$. In these two talks, I will describe an approach which led to a rigorous proof of this result and other related ones, and which, as pointed out above, relied on recent work on spectral estimates for Markov processes motivated by combinatorial problems. These talks, which are accessible to non-physicists, are intended to describe an example in which ideas from theoretical computer science and probability theory have proved useful in statistical mechanics. The first talk will present the necessary background on the stochastic Ising model, and the second will develop the results in some detail.

- **J.J. Seidel (Technical University, Eindhoven):**
  Banach and designs

  Isometric embeddings of Euclidean into Banach spaces are related to Cubature formulae and to designs in Euclidean spaces. This main theorem, due to Reznick and to Lyubich-Vaserstein, brings together objects from various mathematical disciplines. The present paper exposes the main theorem, and surveys the objects and their relations.

- **Greg Sorkin (IBM Hawthorn):**
  Simulated annealing for graph bisection

  We resolve in the affirmative a question of Boppana and Bui: whether simulated annealing can, with high probability and in polynomial time, find the optimal bisection of a random graph in $\mathcal{G}_{npr}$ when $p - r = \Theta(n^{\Delta-2})$ for $\Delta \leq 2$. (The random graph model $\mathcal{G}_{npr}$ specifies a "planted" bisection of density r, separating two $n/2$-vertex subsets of higher density p.) We show that simulated "annealing" at an appropriate fixed temperature (i.e., the Metropolis algorithm) finds the unique smallest bisection in $\mathcal{O}(n^{2+\epsilon})$ steps with very high probability, provided $\Delta > 11/6$. (By using a slightly modified neighbourhood structure, the number of steps can be reduced to $\mathcal{O}(n^{1+\epsilon})$.) We leave open the question of whether annealing is effective for Δ in the range $3/2 < \Delta \leq 11/6$, whose lower limit represents the threshold at which the planted bisection becomes lost amongst other random small bisections. It remains open whether hillclimbing (i.e., annealing at temperature 0) solves the same problem.

- **Leen Stougie (University of Amsterdam):**
  Greedy algorithms for the multiknapsack problem

  A class of greedy algorithms is proposed for the solution of the {0,1} multi-knapsack problem. Items are selected according to decreasing ratios of their profit and a weighted sum of their requirement coefficients. The solution obtained is dependent on the choice of the weights. The complexity of computing the set of weights that gives the maximum greedy solution value is considered, and a worst-case performance bound is derived. Based on a probabilistic analysis of the optimal solution value of the problem, a set of weights is determined that yields greedy solutions whose values converge with probability 1, in a relative sense, to the optimal one. The probabilistic analysis of the optimal solution value and of the performance of the greedy algorithm depends heavily on results from the combinatorial approach to empirical process theory.

- **Audrey Terras (UC San Diego):**
  Finite upper half plane graphs are Ramanujan

  We produce some explicit Ramanujan graphs by studying analogs of the Poincare upper half plane. The adjacency operators of our graphs turn out to be mean-value operators on G/K, where $G = GL(2, F)$, F is a finite field, and K is the subgroup of matrices fixing the origin of the upper half plane. Thus, by a general fact about spherical functions on

symmetric spaces, the eigenvalues are the eigenfunctions. Using work of J. Soto-Andrade, this leads to explicit exponential sums giving the spectrum of the adjacency operators of our graphs. These exponential sums have been estimated by N. Katz and, independently, by Winnie Li. The result is that the graphs are Ramanujan.
(Joint work with J. Angel, N. Celniker, S. Poulos, C. Trimble and E. Velasquez)

- **Prasad Tetali (AT&T Bell Labs):**
  Extensions of resistive identities and applications

  Random walks are well known to play a crucial role in the design of randomized off-line as well as on-line algorithms. In this work we prove some basic identities for ergodic Markov chains. Under reversibility, these imply known identities on resistive networks. Besides providing new insight into random walks on (directed) graphs, we show how these identities give us a way of designing competitive randomized on-line algorithms for certain well known problems. As a special case we prove results for undirected graphs, as studied by previous researchers.

- **Ugo Vaccaro (Salerno)**
  Randomness in distribution protocols

  Randomness is a useful computational resource, due to its ability to enhance the capabilities of other resources. Its interaction with resources such as time, space, interaction with provers, as well as its role in several other areas has been studied extensively. In this paper we give a systematic analysis of randomness in secret sharing schemes and in secure key distribution schemes. For secret sharing schemes, we give both upper and lower bounds on the amount of randomness needed; such bounds match for several classes of secret sharing schemes. For secure key distribution schemes, we provide a lower bound on the randomness needed and we show that a recently proposed protocol is optimal with respect to the amount of randomness used.

- **Avi Wigderson (Hebrew University, Jerusalem):**
  Computational pseudo-randomness: a survey

  "Theorem": If it is "hard" to compute exactly the permanent of dense matrices, then it is "easy" to deterministically approximate the permanent of dense matrices.
  The talk will survey the evolution of ideas relating the intractability of natural problems to the computational power of randomness, one consequence of which is the above "theorem."

- **David Zuckermann (MIT):**
  Expanders that beat the eigenvalue bound, and general weak random sources

We describe two applications of an extractor construction. An extractor is an algorithm that extracts random bits from a defective, or weak, random source, using a small number of additional random bits. The first application is to efficiently simulate randomized algorithms using a general weak random source, without any additional random bits. The second application is to efficiently construct graphs on n vertices such that any two subsets of size a share an edge. These expander graphs have a nearly-optimal number of edges, $n^{1+o(1)}/a$, and can be used to give nearly-optimal algorithms for sorting and selecting in rounds, constructing depth 2 superconcentrators, and constructing non-blocking networks. (The extractor construction is joint work with Noam Nisan, and the expander construction is joint work with Avi Wigderson.)

5 RAND Seminars (Bonn)

July 9, 1993:
Probabilistic Algorithms in Inductive Inference Freitag
(Rusins Freivalds)

July 12, 1993:
Fast and Sensitive Searches of Protein Sequence Databases on MIMD Parallel Computers with Distributed Memory
(Reinhard Schneider)

November 5, 1993:
Optimal $\mathcal{O}(1)$–time Randomized Parallel String–Matching
(Wojciech Rytter)

November 19, 1993:
On Representations by Low–Degree Polynomials
(Roman Smolensky)

December 13, 1993:
Computing the Treewidth and Pathwidth of Graphs
(Dieter Kratsch)

December 17, 1993:
Random graph orders
(Graham Brightwell)

January 21, 1994:
Asymptotische Eigenschaften H–freier Graphen
(Angelika Steger)

6 Conferences and Workshops attended (Paris)

- Dagstuhl Workshop on "Average–case Analysis of Algorithms", July 1993
(W. Fernandez de la Vega)

- ICMS Workshop on "Randomness and Computation", Edinburgh, July 26–30, 1993 (see section 4)
- 6^{th} International Seminar on "Random Graphs", Poznan, August 1993 (W. Fernandez de la Vega)
- Oberwolfach Workshop on "Random Structures", August 30 – September 3, 1993
- 1^{st} European Symposium on Algorithms, Bonn, Germany, September 1993
(M. Santha)
- Dagstuhl Workshop on "Computational Convexity", December 6–10, 1993
- 11^{th} STACS, Caen, France, February 1994
(M. Santha)
- Oxford Workshop on "Randomized Algorithms" (RAND), March 1994 (S. Boucheron, W. Fernandez de la Vega, and M. Santha) (see section 3)
- Conference on "Combinatorial Optimization", Amsterdam, April 5–8, 1994 (CO '94)
- Dagstuhl Workshop on "Random Graphs and Related methods", April 11–15, 1994

7 Invited Talks (Oxford)

September 1993:
Randomized approximation schemes for Tutte Gräthendieck invariants.
(IMA/Minneapolis)

September 1993:
The random cluster model.
(University of Minnesota)

November 1993:
Polynomials of graphs, codes and knots.
(University of Exeter)

December 1993:
Randomised Counting Problems.
(Dagstuhl Workshop on Complexity of Counting)

January 1994:
Complexity of colouring: Invariant Society.

March 1994:
Oberwolfach Special Workshop on Approximation Algorithms.

March 1994:
Knots: The Open University.

May 1994:
Matroids: Basics and Problems.
(2 lectures at Trento Workshop on Discrete Optimization)

8 Visitors: Lectures and Technical Discussions (Oxford)

- **Laszlo Babai (University of Chicago and Eotvos University):**
  Multiparty Communication Complexity
- **Anna Karlin (DEC):**
  Competitive Analysis of Some On–line Algorithms Against a Statistical Adversary
- **Eli Upfal (Weizmann Institute):**
  Expander Graphs and Fault Tolerance Computing
- **Moni Naor (Weizmann Institute):**
  What Can Be Computed Locally?
- **Gyula Katona (Hungarian Academy of Sciences):**
  Nearly regular graphs with greedy construction
- **Tandy Warnow (University of Pennsylvania):**
  Inferring Trees from Inexact Distance Data

□