ESPRIT BR Working Group – 7097 (RAND)

Final Report

July 24, 1992 – July 23, 1995

Contents

1 **Overview** 2

2 **Research Papers** 2

3 **RAND Workshops** 15

3.1 Bonn Workshop on Randomized Algorithms (RAND) 15

3.2 ICMS Workshop Randomness and Computation, Edinburgh . . . 21

3.3 Oxford Workshop on Randomized Algorithms (RAND) 32

3.4 Orsay Workshop on Randomized Algorithms 41

3.5 Lund Workshop On Randomized Algorithms (RAND) 51

4 **RAND Seminars (Bonn)** 53

5 **Conferences and Workshops attended (Paris)** 54

6 **Invited Talks (Oxford)** 56

7 **Visitors: Lectures and Technical Discussions** 57

8 Other activities **57**

9 Final Reports **57**

9.1 Edinburgh Site 57

9.2 Leeds Site 60

9.3 Lund University 63

9.4 Oxford 69

9.5 Paris 73

1 Overview

The research within Working Group RAND was conducted in the following research areas:

(1) Design of Efficient Randomized Algorithms,

(2) Foundations of Randomized Complexity of Computational Problems,

(3) Randomized Approximations Algorithms,

(4) Computation with Limited Randomness Resources, Derandomizing Algorithms

(5) Computational Learning Theory.

The list of papers, workshops, and seminars given in the next sections gives an account of the activities of the ESPRIT BR Working Group – 7097 (RAND) in the time between July, 1992 - July, 1995.

2 Research Papers

(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.:
The complexity of coefficients of the Tutte polynomial
to be published in *Discrete Math.*

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

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

(6) 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

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

(8) 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.

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

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

(11) 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.

(12) 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.

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

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

(15) 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.

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

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

(18) 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

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

(20) 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.

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

(22) 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.

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

(24) 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.

(25) 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.

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

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

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

(29) 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.

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

(31) 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

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

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

(34) 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

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

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

(37) 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*

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

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

(40) Grigoriev, D., 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

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

(42) 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.

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

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

(45) 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.

(46) 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*

(47) 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.

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

(49) 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*

(50) 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 80th Birthday, (B. Bollobás, ed.)*

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

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

(53) 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

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

(55) 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*

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

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

(58) Karpinski, Arora, S., Karger, D.:
Polynomial Time Approximation Schemas for Dense Instances of NP-Hard Problems,
Proceedings of the 27th ACM STOC (1995), pp. 284-293.

(59) Karpinski, Cucker, F., Koiran, P., Lickteig, T., Werther, K.:
Proceedings of the 27th ACM STOC (1995), pp. 335-342.

(60) 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.

(61) 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.

(62) 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.

(63) Karpinski, M., Freivalds, R.:
Lower Time Bounds for Randomized Computation,
Proceedings of the 27th ICALP '95, pp. 183-195.

(64) Karpinski, M., Grigoriev, D., Meyer auf der Heide, F., Smolensky, R.:
A Lower Bound for Randomized Algebraic Decision Trees,
to appear in *Proceedings of the 28th ACM STOC (1996).*

(65) 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.

(66) Karpinski, M., Grigoriev, D., Vorobjov, N.:
Lower Bound on Testing Membership to a Polyhedron by Algebraic Decision Trees,
Proceedings of the 36th IEEE (1995), pp. 258-265.

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

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

(69) Karpinski, M., Macintyre, A.:
Polynomial Bounds for VC-Dimension of Sigmoidal and General Pfaffian Neural Networks,
to appear in *J. Computer Systems Sciences, 1996.*

(70) Karpinski, M., Rytter, W.:
Alphabet Independent Optimal Parallel Search for Three-Dimensional Patterns, Revised Version, Research Report No. 85138–CS, Institut für Informatik, Universität Bonn, 1995

(71) 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.

(72) 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.

(73) Karpinski, Rytter, W., Shinohara, A.:
An Improved Pattern-Matching Algorithm for Strings with short Description,
Proceedings of the 6th Symposium on Combinatorial Pattern Matching .

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

(75) 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.

(76) 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.

(77) 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.

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

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

(80) 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

(81) 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 5th Canadian Conference on Computational Geometry*, Waterloo, 1993

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(108) 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*

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

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

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

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

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

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

(115) 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*

(116) Sinclair, A.:.
Improved Bounds for Mixing Rates of Markov Chains and Multicommodity Flow

Combinatorics, Probability and Computing, vol. 1, December 1992, pp. 351–370

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

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

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

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

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

(122) 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

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

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

(125) 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.

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

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

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

(129) Welsh, D.J.A.:
The Random Cluster Process,
in *Discrete Mathematics* *136* *(1994)*, pp. 373–390.

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

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

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

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

(134) 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

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

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

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

3 RAND Workshops

3.1 Bonn Workshop on Randomized Algorithms (RAND)
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 (March 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 $\mathbb{R}^{\ltimes}$ 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.

3.2 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.

[1] International Centre for Mathematical Sciences, Edinburgh

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

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 $\mathbb{Z}$. 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 $\mathbb{Z}$, 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.)

3.3 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 $A \in \mathrm{Age}(M)$ (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/ Universit"at 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 $H \in \mathcal{H}$, $\text{mindeg}(H) = (1 - o(1))\text{maxdeg}(H)$ and $\text{maxcodeg}(H) = o(\text{maxdeg}(H))$ then H contains
  $$\exp\left\{(1 + o(1))\frac{|V(H)|}{k} \ln \text{ maxdeg } (H)\right\}$$
  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 $\mathrm{dom}(f) \wedge \mathrm{dom}(g)$.

  (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.

3.4 Orsay Workshop on Randomized Algorithms, October 5–7, 1994

3.4.1 Abstracts of Talks

- **Farid Ablayev, Kazan University, Russia**
  Lower Bounds for One-way Probabilistic Communication Complexity

  We prove three different types of complexity lower bounds for the one-way unbounded-error and bounded-error error probabilistic communication protocols for boolean functions. The lower bounds are proved for

arbitrary boolean functions in the common way in terms of the deterministic communication complexity of functions and in terms of the notion "probabilistic communication characteristic" that we define.

It is shown that for almost all boolean functions either the Yao's lower bound or the first or the third lower bound are more precise depending on the value of probability error.

We present boolean functions with the different probabilistic communication characteristics which demonstrates that each of these lower bounds can be more precise than the others depending on the probabilistic communication characteristics of a function. The examples of boolean functions show that the lower bounds of the paper are precise and incomparable.

Our lower bounds are good enough for proving proper hierarchies for various one-way probabilistic communication complexity classes (namely for unbounded error probabilistic communication, for bounded error probabilistic communication, and for errors of probabilistic communication).

- **Arne Andersso,Lund Universityn**
  On the relation between entropy and time complexity

  We present a new randomized sorting algorithm, Forward Radix Sort. The complexity of the algorithm may be expressed in terms of the expected number of characters (or bits) that need to be inspected in order to tell the sorted items apart. It may also be analyzed in terms of random input from a stationary ergodic source with a certain entropy, a model commonly used in information theory.

- **Gilles Brassard, Montréal**
  Quantum Cryptography

  Classical and quantum information are very different. Classical information can be read, copied, and transcribed into any medium; it can be transmitted and broadcast, but it cannot travel faster than the speed of light. Quantum information cannot be read or copied without disturbing it, but in some instances it seems to propagate instantaneously or even backward in time. Together the two kinds of information can perform several feats that neither could achieve alone. These include quantum cryptographic systems, some of which have already been built, in which the privacy of communications is guaranteed by Heisenberg's uncertainty principle. Quantum cryptography allows two parties who have never met and who share no secret information beforehand to communicate in absolute secrecy under the nose of an adversary, regardless of the adversary's computing power. Quantum techniques may also assist in the achievement of subtler cryptographic goals, such as protecting private information while it is being used to reach public decisions.

- **Claude Crépeau, Montréal**
  Generalized Privacy Amplification

  This work provides a general treatment of privacy amplification by public discussion, a concept introduced by Bennett, Brassard and Robert. It is concerned with unconditionally-secure secret-key agreement by two communicating parties Alice and Bob who both know a random variable W, for instance a random n–bit string, about which an eavesdropper Eve has incomplete information characterized by the random variable V jointly distributed with W according to P_{VW}. This distribution may partially be under Eve's control. Alice and Bob know nothing about P_{VW}, except that it satisfies a certain constraint.

  We present protocols by which Alice and Bob can use a public channel, which is totally susceptible to eavesdropping by Eve, to agree on a function $g : \{0,1\}^n \to \{0,1\}^r$ such that Eve, despite her partial knowledge about W and complete knowledge about g, almost certainly knows nearly nothing about the secret key $g(W)$. We characterize how the size r of the secret they can safely distill depends on the kind and amount of Eve's partial information on W.

  The results have applications to unconditionally-secure secret-key agreement protocols, quantum cryptography and to a non-asymptotic and constructive treatment of the secrecy capacity of wire-tap and broadcast channels, even for a considerably strengthened definition of secrecy capacity.

- **Alain Denise, Bordeaux**
  Random uniform generation of rooted planar maps

  The subject of this work is the uniform generation of random rooted planar maps with n edges. A planar map is the projection of a planar connected graph on a plane surface. A map is rooted if a vertex and an edge adjacent to it are distinguished. Thanks to an encoding of planar maps due to Cori and Vauquelin [3], we reduce the problem to a problem of generation of words of a language close to the language of parenthesis systems. Then we generate these words by using an improved rejection algorithm, inspired by the methods of Barcucci, Pinzani and Sprugnoli [1, 2]. We prove that the average complexity is $O(n^2)$, and we conjecture that it may be improved to $O(n\sqrt{n})$.

References

[1] E. Barcucci, R. Pinzani, and R. Sprugnoli. Génération aléatoire des animaux dirigés. In J. Labelle and J. G. Penaud, editors, *Actes de l'Atelier Franco-Québécois de Combinatoire*. Publi LaCIM 10, Université du Québec à Montréal, 1991.

[2] E. Barcucci, R. Pinzani, and R. Sprugnoli. The random generation of underdiagonal walks. In P. Leroux and C. Reutenauer, editors, *Proceedings of the 4th Conference on Formal Power Series and Algebraic Combinatorics*. Publi LaCIM 11, Université du Québec à Montréal, 1992.

[3] R. Cori and B. Vauquelin. Planar maps are well labeled trees. *Can. J. Math.*, 33(5):1023–1042, 1981.

- **Martin Dyer, Leeds**

  Generating a random vertex of a polyhedron

  We consider the problem of generating a random vertex of a polyhedron defined by a unimodular constraint system. We will argue that this problem is a common generalisation of some open problems in this area. We will describe an approach which gives some preliminary results.

- **Jeff Edmonds**

  Probabilistic Erasure Codes

  The Priority Encoding Transmission Scheme (PET) is described in an earlier talk. The basic building blocks of this scheme are erasure codes. Erasure codes encode messages consisting of b words into encodings consisting of n words. The code has the property that all b words of the message can be recovered from any b words of the code. These codes can be implemented easily using polynomial evaluation and interpolation. The problem is that the computation time required is $O(b^2)$. Because the message is of size b, the overhead (time/word) is $O(b)$. For large values of b this may turn out to be infeasible. In this talk, we present a probabilistic erasure code whose computation time is much less. The encoding is probabilistic in the sense that given any $(1+\delta)b$ words of the code, the message can be decoded with some probability depending only on δ. The basic idea is to break the message into small pieces, called bundles. These bundles are in turn be broken into smaller bundles. This forms a hierarchy of bundles. Each word of the encoding $E(M)$ will contain information about a randomly chosen bundle of a randomly chosen size. In order to recover a bundle, the number of words received about it or about one of its sub-bounds must be at least the number of words in the bundle itself. Calculating the probability of this leads to an interesting question in probability theory. The computation time for the encoding and the decoding is much less than for the deterministic erasure codes. In the deterministic code, the overhead was $O(b)$ because each word of the code contains information about all b words of the message. Now they only contain information about one small bundle. Hence, the overhead (time/word) is only the average bundle size.

- **Abdelhakim El-Maftouh, Paris**
  Balance in random signed graphs

  A random signed graph is a graph obtained from the usual random graph $G(n, 2p)$ with edge probability $2p$, p fixed, by assigning to each edge either the plus or the minus sign with probabilities both equal to $1/2$. A signed graph is balanced if the number of negative edges in each cycle is even. We show that $p = \frac{1}{n}$ is the threshold for balance in a random signed graph. We also show that for p constant, the maximum size of a largest induced balanced subgraph of a random signed graph is asymptotically almost surely equal to $2\log_d n - 2\log_d \log_d n + O(1)$, where $d = \frac{1}{1-p}$. Other parameters of these graphs are examined.

- **W. Fernandez de la Vega, Paris**
  A Randomized Approximation Scheme for MAX CUT in Dense Graphs

  A cut in a graph $G = (V(G), E(G))$ is the boundary $\delta(S)$ of some subset $S \subseteq V(G)$ and the maximum cut problem for G is to find the maximum number of edges in a cut of G. Let $\mathrm{MC}(G)$ denote this maximum.

  For any given $\alpha > 0$, $\epsilon > 0$ and $q < 1$, we give a randomized algorithm which runs in polynomial time and which, when applied to a graph G on n vertices with at least αn^2 edges, outputs a number $S \leq MC(G)$ with $P[S \geq \mathrm{MC}(G)(1-\epsilon)] \geq q$.

- **Torben Hagerup**
  Parallel Randomized Sorting

  We will go sightseeing in the scenic spot formed by the intersection of the areas of parallel algorithms, randomized algorithms, and sorting. No new results will be presented, but simpler proofs of old results will be attempted, and different results will be put in relation to each other. We begin with general (comparison-based) sorting, proceed through integer sorting and end, time permitting, with a brief excursion to sorting independent random numbers. The emphasis will be on results, methods and open problems, less on technical details.

- **Alexander Hufnagel, Trier**
  (mixed) Volumes of Convex bodies

  A theorem of Minkowski shows that for convex bodies $K_1, K_2, \ldots, K_s$ and nonnegative reals $\lambda_1, \lambda_2, \ldots, \lambda_s$, the n-dimensional volume $(\sum_{i=1}^{s} \lambda_i K_i)$ of the *Minkowki-sum* $\lambda_1 K_1 + \ldots + \lambda_s K_s$ is a homogeneous polynomial of degree n in $\lambda_1, \ldots, \lambda_s$, and can be written in the form $(\sum_{i=1}^{s} \lambda_i K_i) = \sum_{i_1=1}^{s} \sum_{i_2=1}^{s} \cdots \sum_{i_n=1}^{s} \lambda_{i_1} \lambda_{i_2} \cdots \lambda_{i_n} V(K_{i_1}, K_{i_2}, \ldots, K_{i_n})$, where the coefficients $V(K_{i_1}, K_{i_2}, \ldots, K_{i_n})$ are order-independent, i.e. invariant under permutations of their arguments.

  The coefficient $V(K_{i_1}, K_{i_2}, \ldots, K_{i_n})$ is called the *mixed volume* of $K_{i_1}, K_{i_2}, \ldots, K_{i_n}$. The corresponding *Brunn-Minkowski* theory is the

backbone of convexity theory, but it is also relevant for numerous applications in combinatorics, algebraic geometry and a number of other areas – some of them will be outlined in the talk.

We first present several #P-hardness results that focus on the difference of computing mixed volumes versus computing the volume of polytopes.

On the positive side we derive a randomized algorithm for computing the mixed volumes $V(\overbrace{K_1,\ldots,K_1}^{m_1},\overbrace{K_2,\ldots,K_2}^{m_2},\ldots,\overbrace{K_s,\ldots,K_s}^{m_s})$ of convex bodies $K_1,\ldots,K_s$, where $m_1,\ldots,m_s \in N$ and $m_1 \geq n-\psi(n)$ with $\psi(n) = o(\frac{\log n}{\log\log n})$. The algorithm is an interpolation method based on polynomial-time randomized algorithms for computing the volume of convex bodies.

Mark Jerrum, Edinburgh
Randomised rounding heuristics for semidefinite programming relaxations

Goemans and Williamson recently introduced a new approach to obtaining approximate solutions to combinatorial optimisation problems. Their idea is to formulate a Semi-Definite Program (SDP) relaxation of the optimisation problem in question, solve the SDP using one of a number of polynomial time algorithms, and recover an approximate solution to the original problem using a randomised rounding heuristic. By applying this approach to the Max Cut problem, they achieved a performance ratio of 0.878, a great advance over the trivial ratio $\frac{1}{2}$ that was the best previously known.

The heuristic of Goemans and Williamson applies to problems formulated in terms of binary variables. The extension to k-valued variables is conceptually straightforward, but the analysis of the heuristic then becomes both more difficult and more interesting. It can be shown that the generalised heuristic achieves a performance ratio for the Max k-Cut problem that uniformly exceeds the trivial $1-k^{-1}$. Similar techniques have been applied by Karger, Motwani and Sudan to the graph colouring problem.

- bf Marek Karpinski, Bonn
  A Lower Space Bound for the Randomized Computation

  We present a new method for proving randomized lower space bounds for the explicit problems at the level $\Omega(\log n)$. This yields the first explicit randomized lower space bounds up to the level $\log n$, and answers the open problem of A. Yao on the lower randomized space bounds for testing equality of strings by fingerprinting (palindromes). This says also that any randomized fingerprinting algorithm for the *pattern matching* necessarily requires $\Omega(\log n)$ space.

- **Mike Luby, Berkeley** *Resilient Video Transmission*

We introduce a novel approach for sending messages over lossy packet-based networks. The new method, called Priority Encoding Transmission, allows a user to specify a different priority on each segment of the message. Based on the priorities, the sender uses the system to encode the segments into packets for transmission. The system ensures recovery of the segments in order of their priority. The priority of a segment determines the minimum number of packets sufficient to recover the segment.

We define a measure for a set of priorities, called the *rate*, which dictates how much information about the message must be contained in each bit of the encoding. We develop systems for implementing any set of priorities with rate equal to one. We also give an information-theoretic proof that there is no system that implements a set of priorities with rate greater than one.

This work has immediate applications to multi-media and high speed networks applications, e.g., for sending audio and video information in real-time multi-cast teleconferencing applications.

Contributers to work: Andres Albanese, Johannes Bloemer, Jeff Edmonds, Madhu Sudan, Malik Kalfane, Christian Leicher.

> *Motivational quotes from lead story of business section of NY Times, Wednesday, September 21, 1994 titled "A Rough Start for Digital TV"*
>
> *Neil Shapiro, self-described video enthusiast, has seen the future face of television, and it is ... blemished.*
>
> *During a basketball game, the ball zipping around the backcourt can look like Halley's comet, with a long orange tail. During a football game, as the camera sweeps the field to follow the arc of the pass, the spectators can turn into solid rectangles of color. And in some parts of the country, a heavy rain during a movie can cause a picture to freeze on a single frame for several minutes, or disappear altogether.*
>
> *But this is the long-awaited digital television, and when the picture is good it's computer perfect.*
>
> *Digital technology is often discussed in terms of its computer-like precision, which makes it much less subject to the static or other interference that can mar the picture in analog broadcasting and cable television pictures. But analog video images tend to degrade only gradually. With digital, when there's a problem, the picture can break up with a jarring abruptness.*

- **Ilan Newman, Haifa**
  POS optical technology as the communication media for distributed and parallel computing

We investigate the use of POS optical technology as the communication media for distributed and parallel computing. The POS is the up growing model for processors interconnection in an optical computer. Essentially, it connects the processors via predescribed broadcasting channels with concurrent read and write. The access to these channels is, however, in an implicit way by tuning to given frequency rather then specifying the destination or source.

A feature of parallel models which is extremely important for the simplicity of algorithm design and program portability is the Brent principle, or the model *scalability*. It states that when a computation achieves a certain speedup on a large machine with many processors, then it achieves a proportional speedup (relative to the number of processors) on any smaller machine.

Does the Brent principle hold for POS optical systems? We show that the answer essentially depends on how much randomness we allow. We present several algorithms and a lower bound. Our positive and negative answers identify several aspects of algorithmic design: off-line vs. online, deterministic vs. randomized, and direct vs. indirect communication.

- **S. E. Nikoletseas, Patras**
  Expander properties in random regular graphs with edge faults

  Let H be an undirected graph. A random graph of type$-H$ is obtained by selecting edges of H independently and with probability p. We can thus represent a *communication network* H in which the links *fail independently* and with probability $f = 1 - p$. A fundamental type of H is the clique of n nodes (leading to the well-known random graph $G_{n,p}$). Another fundamental type of H is a *random member* of the set G_n^d of all regular graphs of degree d (leading to a new type of random graphs, of the class $G_{n,p}^d$). Note that $G_{n,p} = G_{n,p}^{n-1}$.

  Information about the remaining (with high probability) structure of type$-H$ random graphs is of interest to applications in reliable network computing. For example, it is well known that any member of G_n^d is almost surely an *efficient certifiable expander*. Expanders are widely used in Computer Science. In a previous work ("Short Vertex Disjoint Paths and Multiconnectivity in Random Graphs: Reliable Network Computing", 21st ICALP, 1994) we have shown that $G_{n,p}^d$ has a *giant component of small diameter* even when $d = O(1)$. We wish to determine the *minimum* value of p for which the giant component of $G_{n,p}^d$ remains a certifiable expander with high probability. In this paper we show that the second eigenvalue of the adjacency matrix of the giant component of $G_{n,p}^d$ is concentrated in an interval of small width around its mean, and that its mean is $O((dp)^{3/4})$, provided that $dp > 256$. Thus, the giant component of a random member of $G_{n,p}^d$ remains, with high probability, a *certifiable efficient expander*, despite the link faults, provided that $dp > 256$.

- **Noam Nisan, Jerusalem**
  Pseudorandomness for Network Algorithms

  We define pseudorandom generators for Yao's two-party communication complexity model and exhibit a simple construction, based on expanders, for it. We then use a recursive composition of such generators to obtain pseudorandom generators that fool distributed network algorithms. While the construction and the proofs are simple, we demonstrate the generality of such generators by giving several applications.

- **Lars Eilstrup Rasmussen, Berkeley** *Extracting Hidden Approximations*

  We present ongoing work on the following topic: Suppose we are given a small set of probabilistic algorithms targeting some counting problem, along with knowledge that for any input, at least one of the algorithms produce a good approximate answer. In which such settings can we (efficiently) extract from the given algorithms a good approximation for any input? What do we need to assume about the counting problem? Or about the faulty estimates?

- **Maria Serna, Barcelona**
  The average complexity of the Circuit Value Problem

  We introduce a uniform model to generate at random boolean circuits that correspond to instances of the Circuit Value Problem. We show that in such a model the expected depth of circuits is logarithmic in the number of gates. Therefore, we can place the monotone circuit value problem in average NC.

- **Jacques Stern, Paris**
  Expansion properties of directed random Schreier graphs of small degree and an application to cryptography

  We show that random directed Schreier graphs S_n/S_{n-k} (where S_n is the set of permutations of n elements) are for fixed k, almost always good expanders. These graphs generalize the common probabilistic model of random regular graphs, for which such kind of results were already known. Nevertheless here we are particularly interested in estimating the expansion constant of directed random graphs, whereas all the known result were obtained for undirected graphs. Moreover our result covers the case of graphs with very low degree, which was not really considered by previous work of A. Broder, J. Friedman, and E. Shamir.

  What motivated our study was a cryptographic issue : it was thought that some low-cost cryptographic devices could be constructed by using permutation automata. We prove here, that the scheme which was proposed is in general not secure, provided that some random directed Schreier

graphs with low degree have good expansion properties. The aforementioned result imply that one could break such schemes by a polynomial time algorithm.

- **Paul Vitanyi, Amsterdam**
  Minimum Description Length from First Principles: Similarity and Difference with Bayes' Rule

  The Minimum Description Length (MDL) criterion is a widely used statistical inference method which selects the hypothesis which minimizes the sum of the length of the description of the hypothesis and the length of the description of the data relative to the hypothesis.

  We derive MDL from first principles using Bayes' rule and a notion of randomness of individual objects. It is shown that MDL is data driven in the sense that it selects a hypothesis with respect to which the given individual data sample is random.

  MDL differs from Bayesian reasoning in case the prior distribution and given data sample give highest posterior probability to a hypothesis against which the data sample is not individually random. We give several applications. The techniques used are based on descriptional complexity (Kolmogorov complexity) and randomness tests in the sense of Martin-Löf.

- **Dominic Welsh, Oxford**
  Polynomial time randomised approximation schemes for Tutte-Gröthendieck invariants

  The Tutte polynomial $T(G;x,y)$ of a graph G encodes numerous interesting combinatorial quantities associated with the graph. Its evaluation in various points in the (x,y) plane give the number of spanning forests of the graph, the number of its strongly connected orientations, the number of its proper k-colourings, the (all terminal) reliability probability of the graph, and various other invariants the exact computation of each of which is well known to be $\#P$-hard. Here I survey the problem of finding a fully polynomial randomised approximation schemes for approximating the value of $T(G;x,y)$. In particular I shall describe recent results obtained with Noga Alon and Alan Frieze which will give an fpras for evaluating T for any dense graph G, that is, any graph on n vertices whose minimum degree is $\Omega(n)$, whenever $x \geq 1$ and $y \geq 1$, and in various additional points. This region includes evaluations of reliability and partition functions of the ferromagnetic Q-state Potts model, and extends to linear matroids where T specialises to the weight enumerator of linear codes.

- **Kai Werther, Bonn**
  Real complexity classes, their Boolean parts, and probabilism

In this talk we consider real analogous of classical probabilistic complexity classes in the framework of real Turing machines as introduced by Blum, Shub, and Smale and their Boolean parts, that is classes of languages of zero-one vectors accepted by these machines. In particular we show that the classes BPP, PP, and also PH and PSPACE are not enlarged by allowing the use of real constants and arithmetic at unit cost provided we restrict branching to equality tests. The proofs of these results are based on randomized simulations using techniques from symbolic computation.

- **David Zuckerman, Austin,Texas**
  Computing with Very Weak Random Sources

  For any fixed $\epsilon > 0$, we show how to simulate RP algorithms in time $n^{O(\log n)}$ using the output of a *ds* with min-entropy R^{ϵ}. Such a weak random source is asked once for R bits; it outputs an R-bit string such that any string has probability at most $2^{-R^{\epsilon}}$. If $\epsilon > 1 - 1/(k+1)$, our BPP simulations take time $n^{O(\log_k n)}$ ($\log_k$ is the logarithm iterated k times). We also give a polynomial-time BPP simulation using Chor-Goldreich sources of min-entropy $R^{\Omega(1)}$, which is optimal. We present applications to time-space tradeoffs, expander constructions, and the hardness of approximation. Also of interest is our randomness-efficient Leftover Hash Lemma, found independently by Goldreich & Wigderson.

3.5 Lund Workshop On Randomized Algorithms (RAND)

Lund University, June 2 - 3, 1995
Building E, Ole Römers väg 3, room 1406

Friday, June 2, 1995

Session 1 (chair A. Lingas)

09:00 - 09:10 Opening

09:15 - 10:15 Rusins Freivalds
Lower Time Bounds for Randomized Computation

10:15 - 10:45 coffee break

Session 2 (chair M. Karpinski)

10:45 - 11:15 Martin Dyer
A randomized parallel convex-hull algorithm

11:15 - 11:45 Andrzej Lingas
Randomized algorithms for polygon skeletons

11:45 - 13:45 lunch break

Session 3 (chair E. Upfal)

13:45 - 14:30 Dominic Welsh
On estimating the number of colorings

14:30 - 15:00 Russ Bubley
Approximately counting the number of k-colorings of a hypergraph

15:00 - 15:30 coffee break

Session 4 (chair C. Levcopoulos)

15:30 - 15:50 Christophe Durr
A decision procedure for well-formed quantum linear cellular automata

18:00 Workshop dinner

Saturday, June 3, 1995

Session 5 (chair D. Welsh)

09:30 - 10:30 Eli Upfal
Balanced allocations

10:30 - 11:00 Bogdan Chlebus
Simulating PRAM in a faulty memory environment

11:00 - 11:30 coffee break

Session 6 (chair M. Dyer)

11:30 - 12:20 Marek Karpinski
VC dimension of Pfaffian networks and a derandomizing application

12:20 - 14:20 lunch break

Session 7 (chair M. Jerrum)

14:20 - 14:50 Vivek Gore
A uniform sampling of words from

an ambigous contex free language

14:50 - 15:20 Boucheron Stephane
About Fourier sampling

15:20 - 15:50 coffee break

Session 8 (chair M. Santha)

15:50 - 16:20 Jingsen Chen
Parallel randomized heap construction

16:20 - 16:40 Alexander Zelikowsky
A new approach to Steiner tree approximation

4 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)

January 9, 1995:
Priority Encoding Transmission
(Johannes Bloemer)

January 11, 1995:
VC Dimension of Sigmoidal Neural Networks
(Angus Macintyre)

January 13, 1995:
Degree of boolean functions over reals and the depth of decision trees
(Roman Smolensky)

May 19, 1995:
Hyperbäume und algorithmische Anwendungen
(Andreas Brandstädt)

June 14, 1995:
Natural Proofs
(Stephen Rudich)

June 23, 1995:
On Line Optimization
(Lawrence Larmore)

June 30, 1995:
Meeting Times of Random Walks on Graphs
(Lisa Higham)

June 30, 1995:
Comparing Evolutionary Trees
(Teresa Przytycka)

5 Conferences and Workshops attended (Paris)

- 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 80th 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)
- 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 3.2)

- 6th International Seminar on "Random Graphs", Poznan, August 1993
  (W. Fernandez de la Vega)
- Oberwolfach Workshop on "Random Structures", August 30 – September 3, 1993
- 1st European Symposium on Algorithms, Bonn, Germany, September 1993
  (M. Santha)
- Dagstuhl Workshop on "Computational Convexity", December 6–10, 1993
- 11th 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 3.3)
- Conference on "Combinatorial Optimization", Amsterdam, April 5–8, 1994 (CO '94)
- Dagstuhl Workshop on "Random Graphs and Related methods", April 11–15, 1994

6 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)

7 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

8 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)).

9 Final Reports

9.1 Edinburgh Site

9.1.1 Esprit Working Group 7097, "RAND"

9.1.2 Report on the Edinburgh Site, 1994–95

Overview of research This brief overview sketches new directions that research at Edinburgh has taken in the past year or so.

For several years now, researchers at Edinburgh—as at a number of other sites both within and outside RAND—have been much concerned with random sampling of combinatorial structures using, in particular, Markov chain simulation. Determining the rate of convergence of the simulated Markov chain to equilibrium is the crucial step in the analysis of such sampling procedures, and in this context the "canonical paths" technique has scored some notable successes. Perhaps because of these successes, we have concentrated on the canonical path method to the exclusion of others.

The past year or two has seen a tentative return to more classical "coupling" methods: a simple application was reported last year in the context of graph colouring, while, more recently, Bubley (Leeds), Dyer (Leeds) and Jerrum (Edinburgh) have applied coupling arguments to Markov chains arising in the estimation of the volume of convex bodies, and the approximation of a certain class of multidimensional integrals. On occasion, we have even avoided Markov chains entirely: in [10], Gore (Edinburgh) and Jerrum build on work of Kannan, Sweedyk and Mahaney, and Karp and Luby, to provide a fairly efficient procedure for sampling words from an (ambiguous) context-free language.

An important development that we have tracked is the use of "semidefinite programming" relaxations allied to "randomised rounding" heuristics to obtain good approximations to problems in combinatorial optimisation, an approach that was pioneered by Goemans and Williamson. Frieze (CMU) and Jerrum [6] contributed to this line of research by providing a possible generalisation of the method from binary to k-valued variables. A similar generalisation was proposed independently by Karger, Motwani and Sudan.

Exploitation of results The theoretical work on Markov chain simulation is coming to maturity, and attention is beginning to turn to practical considerations. The potential applications are wide ranging: in statistical physics (estimating the expectation of various random variables with respect to the Gibbs distribution), image analysis (image reconstruction), and multidimensional integration of certain classes of functions. Dyer, Frieze, Kannan, Lovász and Simonovits (in various combinations) have considered the latter problem, bringing down the exponent governing the run-time from its early, impossibly large value, to something close to usable. In general, it must be admitted, the *provable* run-times of algorithms based on Markov chain simulation are still too high for practical applicability.

The problem to be faced is that a relatively large number of steps of the simulation must be performed in order to *guarantee* that the process is close to equilibrium. One suspects that the theoretical upper bounds on convergence time are very pessimistic, certainly in specific cases, and probably even in general. It would be much better to take an adaptive approach in which the Markov chain is simulated until it is observed to be close to equilibrium; however, there is no direct way of telling when this has occurred.

Recently, Propp and Wilson[2] have shown how the simulation may sometimes be modified so that it becomes easy to recognise when convergence has taken place. In realistic examples, convergence occurs more rapidly than the known theoretical bounds would suggest. Propp and Wilson's idea opens the door to a class of randomised algorithms that are empirically fast, but for which no practically useful *a priori* bound can be placed of the run-time. Such algorithms might be acceptable in many practical situations, and offer a plausible route to realising the potential of the theoretical work.

Personnel Mark Jerrum, Vivek Gore (faculty, since September 1994), Jitka Stříbrná (postgraduate student, since October 1994).

Publications (since July 1994)

(1) Leslie Ann Goldberg, Mark Jerrum, and Philip D. MacKenzie, An $\Omega(\sqrt{\log\log n})$ lower bound for routing in optical networks, *Proceedings of the 6th ACM Symposium on Parallel Algorithms and Architectures* (1994), pp. 147–156.

(2) Mark Jerrum, Counting trees in a graph is #P-complete. *Information Processing Letters* **51** (1994), pp. 111-116.

(3) Robert W. Irving and Mark R. Jerrum, *3-D statistical data security problems*, *SIAM Journal on Computation* **23** (1994), pp. 170-184.

(4) Mark Jerrum, Simple translation-invariant concepts are hard to learn, *Information and Computation* **113** (1994), pp 300–311.

(5) Yoram Hirshfeld, Mark Jerrum, and Faron Moller, A polynomial-time algorithm for deciding equivalence of normed context-free processes, *Proceedings of the 35th IEEE Symposium on Foundations of Computer Science*, IEEE Computer Society Press, 1994, pp. 623–631.

(6) Alan Frieze and Mark Jerrum, Improved approximation algorithms for MAX k-CUT and MAX BISECTION, *Proceedings of the fourth Integer Programming and Combinatorial Optimization Conference* (IPCO4), Springer-Verlag Lecture Notes in Computer Science **920**, 1995, pp. 1–13.

(7) Mark Jerrum, *The computational complexity of counting*, Report ECS-LFCS-94-296, Department of Computer Science, University of Edinburgh, July 1994. (To appear in the proceedings of the *International Congress of Mathematicians*, Zürich, August 1994.)

(8) Mark Jerrum, Computational Pólya Theory, *Surveys in Combinatorics 1995, London Mathematical Society Lecture Note Series* **218**, Cambridge University Press, 1995, pp. 103–118.

[2] J. Propp and D. Wilson, *Exact sampling using coupled Markov chains and applications to statistical mechanics.* Preprint, 1995.

(9) Alan Frieze and Mark Jerrum, An analysis of a Monte Carlo algorithm for estimating the permanent, *Combinatorica* **15** (1995), pp. 67–83.

(10) Vivek Gore and Mark Jerrum, *A quasi-polynomial-time algorithm for sampling words from a context-free language.* Report ECS-LFCS-95-326, Department of Computer Science, University of Edinburgh, July 1995.

(11) Paul Goldberg and Mark Jerrum, Bounding the Vapnik-Chervonenkis dimension of concept classes parameterized by real numbers, *Machine Learning* **18** (1995), pp. 131–148.

(12) Mark Jerrum, The "Markov chain Monte Carlo" method: analytical techniques and applications, *Complex Stochastic Systems and Engineering*, D. M. Titterington (ed.), IMA Conference Series volume **54**, Oxford University Press, 1995, pp. 191–207.

Conferences/workshops attended (since July 1994)

(1) International Congress of Mathematicians, Zürich, August 1994. Jerrum (invited speaker).

(2) Research programme/workshop at Aarhus, Denmark, August 1994. Jerrum (invited speaker).

(3) RAND Meeting, Gif-sur-Yvette, France, October 1994. Gore, Jerrum (contributed talk).

(4) British Mathematical Colloquium, Heriot-Watt, Edinburgh, April 1995. Jerrum (invited speaker).

(5) One-Day Combinatorics Colloquium, Reading, May 1995. Jerrum (invited speaker).

(6) Fourth IPCO (Integer Programming and Combinatorial Optimization) Conference, Copenhagen, May 1995. Jerrum (contributed talk)

(7) RAND Meeting, Lund, June 1995. Gore (contributed talk), Jerrum.

(8) British Combinatorial Conference, Stirling, July 1995. Gore, Jerrum (invited speaker).

9.2 Leeds Site

Site contact: Professor Martin Dyer
School of Computer Studies
University of Leeds
Leeds LS2 9JT
UK

Tel: +44-113-2335442
e-mail: dyer@scs.leeds.ac.uk

9.2.1 Introduction

The principal objective of the RAND work at Leeds was to study the impact of randomized methods in areas of computer application. There was also an objective to obtain more fundamental understanding of the difficulties of combinatorial counting problems. Most of the work performed under the grant was carried out by Martin Dyer in collaboration with researchers at RAND and RAND-REC sites. Two other Leeds researchers have been involved, Russ Bubley, a graduate student who commenced his studies in October 1994, and Jonathan Nash, a research associate working in the area of parallel computation. A description of the work carried out by the Leeds site is given in section 9.2.2. Some conclusions are given in section 9.2.3. Since this is largely theoretical work, the main exploitation has been in the production of conference and journal publications. A list of publications arising from the work is given in section 9.2.4.

9.2.2 Work Done by the Leeds RAND Site

The emphasis of our effort in the past three years has been in randomized methods for problems of counting and related problems, combinatorial optimization, parallel algorithms and computational biology. We have obtained interesting results in all these areas, and these will be followed up.

Counting and Related Problems With Frieze and Jerrum, we showed the existence of a polynomial time algorithm for counting Hamilton cycles in a dense graph. This problem had been open for some years. With Frieze, Kannan *et al*, we obtained the best result to date for counting the number of solutions to a knapsack problem. With Jerrum and Bubley, we have derived a coupling analysis of a modified form of the Lovász-Simonovits form of random walk for volume computation. This greatly simplifies the analysis, no eigenvalue estimations being required to show rapid mixing.

Combinatorial Optimization With Frieze, we obtained a randomized simplex algorithm for unimodular linear programs. In particular, this established a polynomial bound on the combinatorial diameter of the polyhedra underlying such linear programs, which was previously unknown. With Aronson, Frieze and Suen, we confirmed a conjecture of Dyer and Frieze about the behaviour of the randomized greedy algorithm for graph matchings. With Frieze, we gave a probabilistic analysis of the generalized assignment problem, showing that

there is an algorithm which runs in polynomial time with high probability for random instances in a well established model. With Frieze and Pittel, we examined the greedy matching algorithm in random graphs. The analysis here is not straightforward, and uses a combination of moment methods with generating functions. With Fenner, Frieze and Thomason, we gave a vastly improved solution to a key distribution problem in cryptology.

Parallel Algorithms We obtained an improved EREW parallel algorithm for fixed dimensional linear programming. With Nash and Dew, we designed and analysed a new randomized parallel algorithm for convex hulls on a more realistic model of parallel computation and showed that its practical performance was good. (The literature on parallel algorithms falls very sharply into theoretical work for PRAM models and more practical work on real machines. The PRAM algorithms appear to be very inefficient in practice.)

Computational Biology With Frieze and Suen, we answered a question of Karp on ordering fragments of DNA in a model of genome reconstruction.

With Frieze and Suen, we solved a problem of Karp and Pevzner on the occurrence of fixed length fragments in a genome.

9.2.3 Conclusions

The work carried out under RAND has explored some interesting ideas. We have obtained new understanding of the way randomization can improve performance guarantees for heuristic methods in our work with Aronson, Frieze, Pittel and Suen. We have extended counting methods in our work with Frieze, Jerrum, Kannan, Kapoor, Perkovic and Vazirani. We have studied how randomization can help with practical parallel computing. We have begun to look at how randomized methods may help in cryptography with Frieze, Fenner and Thomason. The RAND working group has provided a valuable environment in which to progress. The work is ongoing, and it is hoped that it will be continued with the help of RAND2, if this is approved.

9.2.4 Publications Arising from RAND

[1] M. E. Dyer and A. M. Frieze, "Probabilistic analysis of the generalised assignment problem", *Mathematical Programming* **55** (1992), 169–181.

[2] M. E. Dyer, A. M. Frieze and B. G. Pittel, "The average performance of the greedy matching algorithm", *Annals of Applied Probability* **3**, 1993, 526–552.

[3] M. E. Dyer, A. M. Frieze, R. Kannan, A. Kapoor, L. Perkovic and U. Vazirani," A mildly exponential time algorithm for approximating the number of solutions to a multidimensional knapsack problem", *Combinatorics, Probability and Computing* **2**, 1993, 271-284.

[4] J. Aronson, M. E. Dyer, A. M. Frieze and S. Suen, "On the greedy heuristic for matchings", *Proceedings of the Fifth Symposium on Discrete Algorithms*, ACM/SIAM Press, 1994, pp 141-149.

[5] M. E. Dyer, A. M. Frieze and S. Suen, "Probability of unique solutions of sequencing by hybridization", *Journal of Computational Biology* **1**, 1994, 105–110.

[6] M. E. Dyer, A. M. Frieze and M. R. Jerrum, *Proceedings of the Fifth Symposium on Discrete Algorithms*, ACM/SIAM Press, 1994, pp 336-343.

[7] M. E. Dyer and A. M. Frieze, "Random walks, totally unimodular matrices and a randomized dual simplex method", *Mathematical Programming* **64**, 1994, 1–16.

[8] M. E. Dyer, "A parallel algorithm for fixed dimensional linear programming", in *Proceedings of the Eleventh Annual Symposium on Computational Geometry*, ACM Press, 1995, pp 345–349.

[9] M. E. Dyer, J. Nash and P. M. Dew, "A randomized convex hull algorithm with good empirical performance", *Proceedings of Symposium on Parallel Algorithms and Architectures*, ACM Press, 1995, pp 21–26.

[10] J. M. Nash, P. M. Dew, M. E. Dyer, "Designing practical parallel algorithms for scalable message passing machines", in WTC'95 World Transputer Congress, IOS Press, 1995, pp 529–544.

[11] M. E. Dyer, A. M. Frieze and S. Suen, "Ordering clone libraries in computational biology", *Journal of Computational Biology* **2**, 1995, 207–218.

[12] M. E. Dyer, T. I. Fenner, A. M. Frieze and A. G. Thomason, "On key storage in secure networks", *Journal of Cryptology*, 1995, to appear.

9.3 Lund University

9.3.1 RAND progress report by the Algorithm Group at the Department of Computer Science at Lund University, 1992-1995

- Address: Department of Computer Science, Box 118, S-221 00 Lund
- Tel: 046 222 45 19 , 046 222 80 30
- Fax: 046 13 10 21

Coordinator

1. Dr. Andrzej Lingas, Professor

- E-mail: andrzej.lingas at dna.lth.se
- Tel: 046 222 45 19

Personnel

2. Dr. Arne Andersson, Assistant Professor, Docent
3. Dr. Rolf Karlsson, Associate Professor
4. Dr. Christos Levcopoulos, Associate Professor
5. Dr. Bengt Nilsson, Assistant Professor
6. Dr. Ola Petersson, Assistant Professor
7. Anders Dessmark, Ph.D. student
8. Oscar Garrido, Ph.D. student
9. Christer Mattsson, Ph.D. student
10. Stefan Nilsson, Ph.D. student
11. Kurt Swansson, Ph.D. student
12. Robert Storlind, Ph.D. student

Key words of the field covered by the group **1. Computational Geometry:**

Voronoi diagrams

Constrained triangulations

Motion planning

Guard problems

2. Sorting and Searching:

Search trees

Hashing

Integer sorting and adaptive sorting

3. Parallel and Sequential Graph Algorithms:

Subgraph and graph isomorphism

k-dependent sets

f-matching

Main results on or related to randomized algorithms and data structures in 92-95 Here we mention only the most important results on or related to randomized algorithms obtained or published by the members of our group in 92-95.

1. Computational Geometry

Voronoi diagrams and related structures. We have designed a linear-time randomized algorithm for the so called bounded Voronoi diagram of a simple polygon [14]. In the diagram the edges of the input figure act as visibility barriers for the vertex sites. Interestingly, we have a linear-time deterministic solution to the corresponding problem in L_1 metric [13]. Further, we have generalized Chew's randomized linear-time algorithm for the Voronoi diagram of a convex polygon to include certain convex hulls in 3D and sequences of monotone line segments in the plane [15]. Recently, we have also obtained a linear-time randomized algorithm for the so called skeleton of a simple polygon, i.e., the Voronoi diagram of the edges of the input polygon [17]. We have also worked on parallel geometric algorithms. For the intriguing open problem of parallel complexity status of the successive hulls problem (not known to be even in RNC), we can report only partial results [8]. On the other hand, we have presented the first nearly work-optimal randomized NC algorithm for the Voronoi diagram of vertices (or, edges) of a convex polygon [16].

2. Data structures

We have designed new efficient data structures for sorting and searching. Randomness is used in two ways, by analyzing algorithms in terms of random input and by employing randomization in the algorithms.

Random input. It is natural to let an algorithm take advantage of the input distribution under the assumption of random input. Such algorithms often prove very fast in practical applications. Recently, we have obtained some highly regarded results in this area. We have presented improved algorithms for dynamic interpolation search [1]. We have also invented a new efficient sorting algorithm, Forward Radix Sort [2]. The algorithm is very simple and extremely fast in practice. A new method for trie compression, level-compressed tries, combines simplicity with efficiency [3,4,5].

Randomization. Recently, we have made a major breakthrough in the area of sorting, and hence also in the area of algorithm theory. We have improved the complexity of the sorting problem dramatically, showing that n integers can be sorted in $O(n \log\log n)$ time [M1,7]. The algorithm is based on a combination of *range reduction* and *packed sorting*. Both parts are deterministic, but randomization (universal hashing) is

used to decrease the space requirement to linear. Another integer sorting algorithm, signature sort, uses a randomized range reduction technique. This algorithm can sort in $O(n)$ time, provided that the wordlength is $\Omega(\log^{2+\epsilon} n)$, $\epsilon > 0$ [7]. Also, we have derived tale estimates for the classical randomized selection method [M3].

3. Graph Algorithms

Parallel graph algorithms. We have considered a natural generalization of a matching called an *f-matching.* An f-matching is a subset of the edge set of a graph such that for each vertex v at most $f(v)$ incident edges are in the subset. We have shown the problem of finding a maximum cardinality f-matching to be in the randomized NC class [10]. Further, we have provided a randomized NC algorithm for constructing a maximal f-matching which is more efficient that our earlier deterministic NC algorithm for this problem [11,12]. We have also considered an analogous natural generalization of independent set problem called *f-dependent set problem.* An f-dependent set is a subset of the set of vertices of a graph such that for each vertex v in the subset at most $f(v)$ other vertices in the subset are adjacent to v. We have provided several deterministic results on the f-dependent set problem [11]. In particular, we have shown that the problem of finding a maximal f-dependent set problem admits an NC algorithm if f is poly-log bounded. It is an open problem whether for unbounded f one could get a randomized or deterministic NC solution here. Surprisingly we have found the latter problem to be essentially equivalent to the major open problem of whether a maximal independent set of a hypergraph can be constructed by a randomized or deterministic NC algorithm (when hyperedge size is constantly bounded a randomized NC solution is known). For the hypergraph problem we have provided an NC solution in the bounded arboricity case [M2].

Future research Our main research activity will concentrate on algorithm design and analysis within computational geometry, data structures and parallel, distributed and sequential graph algorithms. A special emphasis will be put on randomized algorithms.

In computational geometry, we plan to research efficient randomized and deterministic algorithms for variants of Voronoi diagrams, triangulations and figure decompositions. Also, we intend to start to work on three dimensional versions and dynamic versions of the above problems (in the dynamic setting, the input objects move with possibly different velocities in possibly different directions). We would also work on motion planning in a realistic context where the moving objects have restricted movement possibilities (e.g., bounded curvature or standard curve segments, and acceleration constraints). Finally,

we plan to attack the open problem of parallel complexity of the successive convex hull problem (not known even to be in RNC).

In data structures, we plan to do research on adaptive sorting, distribution-sensitive algorithms and simple algorithms that can efficiently be implemented on real computers. On the other hand, using our expertise in string data structures, we intend to take part in research on biological computing involving algorithms handling large sets of strings.

In graph algorithms, we intend to attack two major open problems in parallel complexity theory: the complexity status of finding maximum matching in a graph (known to be in RNC), and finding a maximal independent set in a hypergraph (not known to be in RNC in general). Also, we would like to combine our expertise on the subgraph isomorphism problem with that on string algorithms to join the research on biological computing.

Selected publications on or related to randomized algorithms of the algorithm group at Lund University in 1992–95

[1] A. Andersson and Ch. Mattsson, *Dynamic interpolation search in* $o(\log\log n)$ *time*, In Proc. ICALP '93, Lecture Notes in Computer Science 700, pp. 15-27, 1993.

[2] A. Andersson and S. Nilsson, *A new efficient radix sort*, In Proc. 35th Annual IEEE Symposium FOCS, 1994.

[3] A. Andersson and S. Nilsson, *Improved behaviour of tries by adaptive branching.* Information Processing Letters 46, pp. 295–300, 1993.

[4] A. Andersson and S. Nilsson, *Efficient implementation of suffix trees.* In Software—Practice and Experience, 1994.

[5] A. Andersson and S. Nilsson, *Faster searching in tries and quadtrees—an analysis of level compression.* In Proc. 2nd Annual European Symposium on Algorithms, Lecture Notes in Computer Science 855, pp. 82-93,1994.

[6] A. Andersson and O. Petersson, co-authors Torben Hagerup and Johan Håstad, *The complexity of searching a sorted array of strings.* Proc. 26th Annual ACM Symposium on Theory of Computing, STOC '94, pp. 317–325, 1994.

[7] A. Andersson, and S. Nilsson, co-authors T. Hagerup, and R. Raman, *Sorting in linear time?* In proc. 27th ACM Symposium on Theory of Computing, 1995.

[8] Anders Dessmark, Andrzej Lingas, co-author A. Maheshwari, *Multi-list ranking: complexity and applications.* Proc. 10th Symposium on Theoretical Aspects of Computer Science, Wurzburg, February 1993, Lecture Notes

in Computer Science 665, pp. 306-316, Springer Verlag. Also, in Theoretical Computer Science 141 (1995) pp. 337-350.

[9] Anders Dessmark and Andrzej Lingas, co-author K. Jansen. *The complexity of maximum k-dependent and f-dependent set.* In proceedings of ISAAC'93, Hong Kong, Lecture Notes in Computer Science , Springer Verlag.

[10] Anders Dessmark, Andrzej Lingas and Oscar Garrido, *On f-Matching and the Degree Sequence Problem.* In Proc. MFCS, August 1994, Lecture Notes in Computer Science 841, Springer Verlag, pp. 316-325.

[11] Oscar Garrido and Andrzej Lingas, co-author K. Diks, *Parallel algorithms for finding maximal k-dependent sets and maximal f-matchings.* Proccedings of the Second Annual International Symposium on Algorithms ISA'91, Taiwan, Lecture Notes in Computer Science 557, pp. 385-396, Springer Verlag. Also, in International Journal of Foundations of Computer Science, 1994.

[12] Oscar Garrido and Andrzej Lingas, co-authors S. Jarominek, W. Rytter, *A simple randomized parallel algorithm for maximal f-matchings*, Proccedings of the International Symposium Latin American Theoretical Informatics LATIN'92. São Paulo - Brazil, Lecture Notes in Computer Science 583, pp. 165-176, Springer Verlag.

[13] Andrzej Lingas, co-author R. Klein. *Manhatanion Proximity in Simple Polygons.* Proc. of the ACM Symposium on Computational Geometry, Berlin, 1992. In the special issue of International Journal of Computational Geometry and Applications, Vol. 5, No. 1-2 (1995) 53-74.

[14] Andrzej Lingas, co-author R. Klein. *A Linear-time Randomized Algorithm for the Bounded Voronoi Diagram of a Simple Polygon.* Proc. of the ACM Symposium on Computational Geometry, San Diego, 1993. To appear in the special issue of International Journal of Computational Geometry.

[15] Andrzej Lingas, co-author R. Klein, *A note on generalizations of Chew's algorithm for the Voronoi diagram of a convex polygon.* Proc. 5th Canadian Conference on Computational Geometry, Waterloo, Canada, 1993.

[16] Andrzej Lingas, co-author P. Berman, *A Nearly Optimal Parallel Algorithm for the Voronoi Diagram of a Convex Polygon.* In Proc. Scandinavian Workshop on Algorithm Theory, July 1994, Lecture Notes in Computer Science 824, Springer Verlag, pp. 73-82.

[17] Andrzej Lingas, co-author R. Klein, *Fast skeleton construction.* Proc. 3rd Annual European Symposium on Algorithms, Lecture Notes in Computer Science 855, pp. 82-93,1994.

Selected manuscripts [M1] A. Andersson, S. Nilsson, co-author T. Hagerup, *Blasting past fusion trees.* Tech. Report, Lund University, 1994.

[M2] O. Garrido, and A. Lingas, *An NC algorithm for a maximal independent set in a hypergraph of poly-log arboricity.*

[M3] C. Levcopoulos, *Tale estimates for selection.*

9.4 Oxford

Report of Oxford group for the year ending 23rd July 1995

Work published or accepted for publication by members of the group in the last year together with research seminars given.

J.D. ANNAN

Topics in computational complexity (thesis). Oxford (1994).

A randomised approximation algorithm for counting the number of forests in dense graphs. *Combinatorics, Probability and Computing* **3** (1994), 135-154.

The complexities of the coefficients of the Tutte polynomial. *Discrete Applied Mathematics* **57** (1995), 93-103.

E. BARTELS AND D.J.A. WELSH

The Markov chain of colourings. *Proceedings of Fourth Conference on Integer Programming and Combinatorial Optimisation (IPCO IV)*, Lecture Notes in Computer Science **920**, Springer (1995), 383-397.

L. CHAVEZ-LOMÉLI

The Basis Problem for Matroids (thesis). Oxford (1994).

P. COWLING

Strong total chromatic numbers of complete hypergraphs, *Discrete Mathematics* **138** (1995), 207-212.

Total colouring of hypergraphs, to appear in the *Journal of Computational Mathematics and Computational Computing.*

C.J.H. MCDIARMID

Sharing jugs of wine, *Discrete Mathematics* **125** (1994), 279-287 (joint with J. Ramirez-Alfonsin).

The complexity of harmonious colouring for trees, *Discrete Applied Mathematics* **57** (1995), 133-144 (joint with Keith Edwards).

On the bandwidth of triangulated cycles, *Discrete Mathematics* **138** (1995), 261-265 (joint with Robert Hochberg and Michael Saks).

On the first birth times for age-dependent branching processes, *Annals of Applied Probability*, to appear.

Centering sequences with bounded differences, *Combinatorics, Probability and Computing*, to appear.

Linear arboricity of random graphs, *Combinatorics, Probability and Computing*, to appear (joint with B. Reed).

Tidier examples for lower bounds on diagonal Ramsey numbers, *J. Combinatorial Theory A*, to appear (joint with Angelika Steger).

D.J.A. WELSH

Randomised approximations in the Tutte plane. *Combinatorics, Probability and Computing* **3** (1994), 137- 143.

The random cluster process. *Discrete Mathematics* **136** (1994), 373-390.

Random generation of polymer configurations. *Probability, Statistics and Optimisation* (ed. F.P. Kelly) (Wiley) (1994), 66-77.

Polynomial time randomised approximation schemes for the Tutte polynomial of dense graphs (Extended Abstract). *Proceedings of 35th Annual Symposium on the Foundations of Computer Science* (1994), 24-35 (with Noga Alon and Alan Frieze).

Randomised approximation schemes for Tutte-Grothendieck invariants. *Proceedings IMA Workshop on Probability and Algorithms*, Univ. of Minnesota (1993) *Discrete Probability and Algorithms* (Springer Verlag) (1995), 133-148.

Matroids, fundamental concepts, *Handbook of Combinatorics* (to be published 1995).

Combinatorics in pure mathematics, *Handbook of Combinatorics* (to be published 1995) (with L. Lovász, L. Pyber and G.M. Ziegler).

Combinatorics in statistical physics, *Handbook of Combinatorics* (to be published 1995) (with C. Godsil and M. Grötschel).

Counting colourings and flows in random graphs. *Bolyai Society Mathematical Studies* **2** (1995) (to appear).

Polynomial time randomised approximation schemes for Tutte- Grothendieck invariants: the dense case. *Random Structures and Algorithms* (1995) (to appear) (with N. Alon and A. Frieze).

Invited Seminars and talks at Workshops

J.D. Farley

6 July 1995	British Combinatorial Meeting, Stirling
	Perfect sequences of chain complete posets

C.J.H. McDiarmid

5 May 1995	Edinburgh Mathematical Society
	Random graph colouring
9 June 1995	15th Berliner Algorithmen Tag
	Random graph colouring
6 July 1995	British Combinatorial Conference, Stirling
	Hypergraph colouring and the Lova'asz Local Lemma

S. Noble

7 July 1995	British Combinatorial Meeting, Stirling
	Evaluating the Tutte polynomial for graphs of bounded

D.J.A. Welsh

8 July 1994	Colloque sur les Arrangements d'Hyperplanes, Marseilles (Luminy)
	The complexity of the Tutte plane
5 October 1994	Rand Workshop Paris-Sud (Orsay)
	Polynomial time randomised approximation schemes for
19 October 1994	School of Physics and Space Research, Birmingham
	NP-hard problems in physics
15 December 1994	Invited lecture at IMA Conference on the Applications of Combinatorial Mathematics
	Algorithmic questions about knots
12 January 1995	Free University, Berlin
	The complexity of polynomials of knots and colourings

University of Bordeaux I (La-Bri)

13 February 1995	*Graphs and knots*
16 February 1995	*The complexity of the Tutte plane*
17 February 1995	*Percolation in the random cluster model*
24 March 1995	*A Markov chain of colourings*
29 March 1995	Colloque "Physique et Combinatoire", Marseilles (Luminy)
	The Markov chain of good colourings
31 May 1995	Fourth IPCO meeting, Copenhagen
	The Markov chain of colourings
2 June 1995	Lund Workshop on Randomised Algorithms
	On estimating the number of colourings
5 July 1995	American Mathematical Society meeting on

Matroids, Seattle

Randomised algorithms for computing numerical

Further Activities

Apart from the activities listed above we have had close cooperation on specific problems with Angelika Steger (Kiel) and Martin Aigner (Berlin), who have both visited Oxford in the past 12 months. There has been close cooperation with the group at Bordeaux I (La Bri) on problems of uniform random generation of combinatorial objects. This is ongoing research which started at the RAND meeting in Oxford in 1994 and is now on the point of producing some interesting computational phenomena. Members of the group have also participated in workshops at Oberwolfach, Dagsthuhl, and Casteljan.

Dominic Welsh
31 July 1995

9.5 Paris

9.5.1 Université Paris-Sud

Conferences and Workshops attended

- Orsay Workshop on "Randomized Algorithms" (RAND), October 1994 (W. Fernandez de la Vega, S. Boucheron, M. Santha, M. de Rougemont)
- Seventh International conference on "Random Structures and Algorithms", Atlanta (USA), May 1995 (W. Fernandez de la Vega)
- FMT (Finite Model Theory), Marseille, April 1995 (M. de Rougemont)
- Logic in weak arithmetic, Mnchen, Germany, June 1995 (M. de Rougemont)
- 12th STACS, Mnchen, Germany, February 95 (C. Drr, H. Le-Thanh, M. Santha)
- Lund Workshop on "Randomized Algorithms" (RAND), June 1995 (S. Boucheron, C. Drr, H. Le-Thanh, M. Santha)
- ISI Workshop on Quantum Computation, Torino, Italy, July 1995 (S. Boucheron)

Visitors: lectures and technical discussions

- N. Nisan (Hebrew University, Jerusalem) : Direct sums, products, and help bits in decision trees and boolean circuits.
- M. Luby (ICSI and UC Berkeley) : Prioriry encoding transmission.
- U. Vazirani (U.C. Berkeley) : Go with the winners.
- P. Hajnal (Budapest) : Randomized complexity on decision trees
- D. Scuciu (Penn State) : Logical characterization of NC.
- E. Grandjean (Universit de Caen) : Dfinissabilit logique et temps linaire (non dterministe)
- S. Khanna (Stanford University) : On syntactic versus computational views of approximability.
- M. Karpinski (Bonn University) : Quadratic Bounds for VC Dimension of Sigmoidal Neural Networks
- R. Jozsa (Plymouth University) : Quantum Computation and Quantum Error Correction
- K. Friedl (Budapest) : On low-degree tests
- P. Koiran (LIP, ENS Lyon) : Modeles de calcul sur les reels, quelques classes de complexite.
- B. Durand (LIP, ENS Lyon) : Rversibilit et automates cellulaires.
- P. Palfy (Hungarian Academy of Sciences, Budapest) : Short Presentations for Finite Groups
- S. Kannan (University of Pennsylvania, Philadelphia) : Introduction to computational biology.
- P. Pezner (Penn State University) : Transforming mice into men and sorting permutations by reversals.
- D. Randall (ICSI Berkeley) : Markov chain algorithms for planar lattice structures.
- M. Luby (ICSI Berkeley) : Linear Time Erasure Codes With Nearly Optimal Recovery.
- C. Kenyon (LIP ENS-Lyon) : Best-Fit Bin-Packing with Random Order

Results are described and discussed according to the work area they fit.

9.5.2 Design and analysis of randomized algorithms

The design and analysis of randomized algorithms may be motivated in different ways: first, it may be the only (known) way to get an efficient (i.e. polynomial or NC) algorithm as it is for primality testing or maximal matching; but it can also be motivated by the desire to improve the worst-case performance of an existing algorithm, as can be checked by randomized quicksort. The last incentive prompts average-case analysis of problems and algorithms.

Average case analysis In [29] it is shown that the running time of the merging algorithm of Hwang and Lin, applied to two ordered lists with lengths m and n, concentrates around its average value when m tends towards ∞, while $\rho = m/n$ is kept constant and distinct from a power of 2. When ρ is a power of 2, the expectation of the running time is obtained. The proof uses martingale methods. The results show that the algorithm of Hwang and Lin is not optimal for certain values of ρ and allow substantial improvements of the algorithm for these values.

Random instances of hard problems Average-case analysis of hard optimization and decision problems became a fashionable topic when powerful probabilistic methods like the bounded difference method became widely spread. But method availability is not the only motivation of that kind of studies: a deeper one is rooted in the fact that the hard instances for some well-respected proof methods like resolution seem to be very oddly spread: it is suspected that they are mostly concentrated around some suspected satisfiability threshold, i.e. when the ratio variable per k-clause in a random instance of k-sat reaches a certain critical value. It should be stressed that for $k \geq 3$, the very existence of such a threshold is still to be established, although it is corroborated by studies in statistical mechanics.

In [21, 23] an exponential lower bound for the number of models of random satisfiable 3-CNF is derived. This lower bound is used to improve the upper bound for the critical value of the ratio (number of clauses/number of variables) that warrants almost sure satisfiability of a random 3-CNF formulae.

Random graphs In [26] the problem of the existence in a random graph of a large subgraph isomorphic to a given graph H of average degree greater or equal than 3 is considered. This kind of problem was treated previously only for subgraphs with average degree 2. The method gives nearly optimal results (up to a logarithmic factor) when H is a grid or a subgraph of the honeycomb lattice and can be applied to many other cases. The proof uses randomized algorithms.

9.5.3 Foundations of randomized complexity

Pseudo-random number generation In cryptography and pseudo-random number generation most results are much easier to establish in the non-uniform model of computation than in the uniform model. In [2] a general framework is proposed in which non-uniform results can be extended to uniform ones under suitable assumptions. The framework is applied to the Schrift-Shamir generalization of the universality of Yao's next-bit-test.

Interactive proofs In [8] direct interactive protocols are given for several graph enumeration and reliability problems. These 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. A new technique is introduced for representing rational probability values in finite fields.

Randomized decision-tree complexity In [35], it is shown that for a large class of read-once balanced formulae, the Las-Vegas and Monte Carlo decision tree complexities are linearly related.

For every formula F belonging to that class we show that the Monte Carlo complexity of F with two sided error p is $(1-2p)R(F)$, and with one sided error p is $(1-p)R(F)$, where $R(F)$ denotes the Las Vegas complexity of F.

Reliability issues In [9], a database oriented generalization of the graph reliability problem is investigated. The hardness of computing the probability that some query will be correctly answered when the answer is computed from a noise corrupted version of an initial database is related to the expressive power of the query language: it is polynomial when the language is first order-logic, and may by #-P-hard when queries are expressed in more expressive languages.

9.5.4 Learning theory

In [5], it is proved that the rate of Vapnik-Chervonenkis entropy associated with a class of sets is a reversed submartingale. This apparently unnoticed fact complements the usual subadditive arguments used to analyze the VC-entropy. The randomized regression rule known as the Gibbs rule has been analyzed. It is shown that the sequence of posterior distributions almost surely converges towards a unique limit law in the high temperature setting , (without any precompactness assumption), whereas in the fixed temperature regime the sequence of posterior laws may oscillate between different accumulation points [4]. A stochastic inference technique known as *input perturbation* has been analyzed and shown to be equivalent to Empirical Risk Minimization under a (kernel)-smoothed density [31].

9.5.5 Randomized approximation problems

In [33] a substancial improvement for the best approximation ratio for the maximum independent set is obtained. In [34], a Boltzmann machine model is defined for solving the maximum independent set and the vertex cover problem. An efficient encoding formalism is proposed and a powerful cooling schedule is shown to be efficient on practically relevant problem instances.

In [20], it is shown that Max-Cut has a randomized polynomial-time approximation scheme on dense graphs. This results, among others, has also been independently obtained by Arora, Karger and Karpinski using related but different methods. It is all the more interesting as the general Max-Cut problem cannot have an approximation scheme unless P=NP.

9.5.6 Quantum computation

Though Quantum Turing Machine and Quantum circuits were defined in the eighties by D. Deutsch, the subject acquired popularity durings the years 1993-1994, when first, the existence of a reasonable universal Quantum Turing Machine was established, and second when it was shown that factoring and discrete log have a polynomial time algorithm on quantum machines. Although formidable obstacles to their construction exist, Quantum Turing Machines appear to be the first challenge to the Polynomial-time version of the Church-Turing thesis. Two kind of problems related to Quantum computations have been considered : questions pertaining to structural complexity and questions concerning the definition of quantum cellular automata.

The structural complexity issues are twofold, first they concern the comparison of the power of natural classes of complexity in the quantum and probabilistic setting. Though quantum computers are believed to be more powerful than classical ones on some problems they are not more powerful on average problems: most boolean functions require exponential-sized quantum circuits [30]. The quantum analogue to BPP, BQP which contains problems like prediction of the hard bits of the discrete log, was only known to be contained in $\mathrm{P}^{\#\mathrm{P}}$ thanks to an unpublished remark by Valiant, in [32], it is shown that $\mathrm{BQP} \subseteq \mathrm{P}^{\Sigma_2^p}$. Finally, its seems that many potentialities provided by Quantum computing are captured by the ability of Quantum computers to perform efficiently a task named Fourier Sampling. The relation between the hardness of this problem and the spectral norm of the function under consideration is established in [6] where it is also shown that Fourier sampling is information-theoretically impossible to perform in polynomial time and powerful in the sense that it enables to solve hard decision problems.

Quantum Cellular Automata are of special interest, in the sense that the construction of QCA may be easier than the construction of Quantum RAMs for deep physical reasons. On the other hand many of the locality constraints that ease the analysis of QTM are no more enforced by the definition of QCA,

hence it was of special interest to develop an algorithm that would recognize whether the transition table of a would-be QCA actually complies with the requirements of Quantum Mechanics, i.e. unitary evolution, this is accomplished in [10], where a polynomial-time algorithm for deciding whether a would-be transition table defines an isometry in the Hilbert space defined by configurations is described.

References

[1] E. Bampis, M. E. Haddad, Y. Manoussakis, and M. Santha. A parallel reduction of hamiltonian cycle to hamiltonian path in tournaments. *Journal of Algorithms*, november 1995. to appear, preliminary version in LNCS 694, page 553-560.

[2] P. Barbaroux. Uniform results in polynomial time security. In *EUROCRYPT 92*, volume 658 of *LNCS*, pages 297–306. Springer Verlag, 1992.

[3] S. Boucheron. *Théorie de l'apprentissage, de l'appoche formelle aux enjeux cognitifs*. Hermès, Paris, 1992.

[4] S. Boucheron. About a maximum entropy methods in learning theory. Manuscript, june 1994. presented at Oxford RAND workshop, and at Workshop on Algorithmic Complexity of Algebraic and Geometric Models, Université paris XII.

[5] S. Boucheron. Sur les traces de l'apprentissage. In A. Gagalowicz and D. Kayser, editors, 9^{éme} *Congrès RFIA*, volume II, pages 1–13. AFCET, 1994. Conférence d'introduction.

[6] S. Boucheron. On the fourier sampling problem. Lund RAND Workshop, june 1995.

[7] S. Boucheron, S. Canu, P. Gallinari, and Y. Grandvalet. De la représentation à la validation : la généralisation dans les réseaux de neurones. In *Actes des* 5ième *journées nationales du PRC Intelligence Artificielle*, pages 397–423. CNRS, Teknea, Février 1995.

[8] J.-M. Couveignes, J. Diaz, M. de Rougemont, and M. Santha. On the interactive complexity of graph reliability. In *14 th Conference on the Foundations of Software Technology and Theoretical Computer Science, LNCS 880*, pages 12–23, 1994. presented at Bonn RAND workshop.

[9] M. de Rougemont. The reliability of queries. *ACM Principles on Databases Systems*, pages 286–291, 1995.

[10] C. Durr, H. Le-Thanh, and M. Santha. A decision procedure for well formed linear quantum cellular automata. Lund RAND Workshop, june 1995.

[11] A. El Maftouhi. The minimum size of a maximal strong matching in a random graph. *The Australasian Journal of Combinatorics*. to appear.

[12] A. El Maftouhi. Irredundancy, Independence and Domination in Random Graphs. *Vishwa International Journal of Graph Theory*, 1(2):149–158, 1992.

[13] A. El Maftouhi. Enumeration of graded orders with fixed width. Random Graphs 93, 1993. Submitted to *Order*.

[14] A. El Maftouhi. *Méthodes Probabilistes en Combinatoire et Théorie des Graphes*. PhD thesis, Université Paris XI, 1994.

[15] A. El Maftouhi. Random graded posets. Communication at the Oxford RAND workshop, march 1994.

[16] A. El Maftouhi. Random signed graphs. Orsay RAND Workshop, October 1994.

[17] A. El Maftouhi and W. Fernandez de la Vega. On random 3-sat. *Probability, Combinatorics and Computing*, to appear.

[18] A. El Maftouhi and L. Marquez Gordonez. The maximum size of a strong matching in a random graph. *The Australasian Journal of Combinatorics*, 10:149–158, 1994.

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

[20] W. Fernandez de la Vega. MAX-CUT has a Randomised Approximation Scheme in Dense Graphs. Orsay RAND Workshop, 1995. submitted.

[21] W. Fernandez de la Vega and A. El Maftouhi. Almost all satisfiable 3-CNF formulas have exponentially many models. Jerusalem Combinatorics Conference, May 1993.

[22] W. Fernandez de la Vega and A. El Maftouhi. On random 2-sat. Communication at Random graphs 93, 1993.

[23] W. Fernandez de la Vega and A. El Maftouhi. On the threshold for the almost sure satisfiability of a random set of 3-clauses. RAND International Workshop: Randomized Algorithms, March 1993.

[24] W. Fernandez de la Vega, S. Kannan, and M. Santha. Two probabilistic results on merging. *SIAM J. Comput.*, 22:261–271, 1993.

[25] W. Fernandez de la Vega and Y. Mannoussakis. On the forwarding index of communication networks with given connectivity. *Annals of Discrete Mathematics*, 37–38:147–155, 1992.

[26] W. Fernandez de la Vega and Y. Manoussakis. Grids in random graphs. *Random Graphs and Discrete Structures*, 5:329–336, 1994.

[27] W. Fernandez de la Vega and L. Marquez Gordones. The forwarding indices of random graphs. *Random Structures and Algorithms*, 3(1):107–116, 1993.

[28] W. Fernandez de la Vega, V. Paschos, and R. Saad. Average case analysis of a greedy heuristic for the minimum hitting set problem. *Theoretical Computer Science*, to appear.

[29] W. Fernandez de la Vega and M. Santha. Average case analysis of the merging algorithm of Hwang and Lin. Fifth Franco-Japanese Days on Combinatorics and Optimization, Kyoto, October 1992.

[30] S. Gonnord. Sur les circuits quantiques. Mémoire de DEA, Université Paris-Sud, Spetember 1995. in french.

[31] Y. Grandvalet, S. Canu, and S. Boucheron. Control of complexity in learning with perturbated inputs. In *Proceedings of 2nd European Symp. on Artificial Neural Networks*, pages 167–74. D facto, 1995.

[32] F. Magniez. Sur le calcul quantique. Mémoire de DEA, Université Paris-Sud, Spetember 1995. in french.

[33] V. Paschos. A $\delta/2$-approximation algorithm for the maximum independent set problem. *Information Processing Letters*, 44, 1992.

[34] V. T. Paschos, F. Pekergin, and V. Zissimopoulos. Approximating the optimal solutions of some hard graph problems by a Boltzmann machine. *Belgian Journal of Operation Research, Statistics and Computer Science*, 1993. to appear.

[35] M. Santha. On the monte carlo decision tree complexity of read-once formulae. *Random Structures and Algorithms*, 6(1):75–87, 1995.

[36] M. Santha and S. Tan. Verifying the determinant in parallel. In *Fifth Annual International Symposium on Algorithms and Computation, LNCS 834*, pages 65–73, 1994.

[37] M. Santha and U. Vazirani. Parallel searching of multi-dimensional cubes. *Discrete Mathematics*, 114:425–443, 1993.

[38] M. Santha and C. Wilson. Polynomial size constant depth circuits with a limited number of negations. *SIAM Journal of Computing*, 22(2):294–302, 1993.

□