Marek Karpinski, Michael Luby,
Umesh Vazirani (editors):

Randomized Algorithms

Dagstuhl-Seminar-Report; 14
10.-14.6.1991 (9124)

ISSN 0940-1121

Das Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI) ist eine gemeinnützige GmbH. Sie veranstaltet regelmäßig wissenschaftliche Seminare, welche nach Antrag der Tagungsleiter und Begutachtung durch das wissenschaftliche Direktorium mit persönlich eingeladenen Gästen durchgeführt werden.

Verantwortlich für das Programm:
Prof. Dr.-Ing. José Encarnaçao,
Prof. Dr. Winfried Görke,
Prof. Dr. Theo Härder,
Dr. Michael Laska,
Prof. Dr. Thomas Lengauer,
Prof. Ph. D. Walter Tichy,
Prof. Dr. Reinhard Wilhelm (wissenschaftlicher Direktor).

Gesellschafter: Universität des Saarlandes,
Universität Kaiserslautern,
Universität Karlsruhe,
Gesellschaft für Informatik e.V., Bonn

Träger: Die Bundesländer Saarland und Rheinland Pfalz.

Bezugsadresse: Geschäftsstelle Schloß Dagstuhl
Informatik, Bau 36
Universität des Saarlandes
W - 6600 Saarbrücken
Germany
Tel.: +49 -681 - 302 - 4396
Fax: +49 -681 - 302 - 4397
e-mail: dagstuhl@dag.uni-sb.de

DAGSTUHL WORKSHOP
ON
RANDOMIZED ALGORITHMS

June 10 – 14, 1991

Organizers:

Marek Karpinski (Bonn)
Michael Luby (Berkeley)
Umesh Vazirani (Berkeley)

MONDAY, 10.6.1991

M. Karpinski (Bonn) :	OPENING SESSION
Y. Mansour (Harvard) :	Learning Decision Trees Using the Fourier Spectrum
D. Zuckerman (Berkeley) :	Simulating Randomized Algorithms with General Weak Random Sources
V. Vazirani (Cornell) :	Fast Parallel Algorithms for Matroid Union Arborescences, and Edge-disjoint Spanning Trees
M. Luby (Berkeley) :	On Deterministic Approximation of DNF / Small Sample Spaces for Nonuniform Random Variables
M. Dyer (Leeds) :	Random Walks on Unimodular Zonotopes
U. Vazirani (Berkeley) :	A Subexponential Algorithm for Approximating the Permanent

TUESDAY, 11.6.1991

A. Shamir (Rehovot) :	Analysis of Multi Prover Protocols
C. P. Schnorr (Frankfurt) :	An Efficient Cryptographic Hash Function
A. Broder (DEC) :	Finding Hidden Hamiltonian Cycles
M. Szegedy (Chicago) :	Randomized On-Line Coloring has Performance Ratio $\frac{n}{\log^3 n}$
A. Steger (Bonn) :	The Kleitman-Rothschild Method and an Application to Perfect Graphs
H.-J. Prömel (Bonn) :	Coloring Clique-Free Graphs in Linear Expected Time

WEDNESDAY, 12.6.1991

M. Santha (Paris) :	On the Monte Carlo Boolean Decision Tree Complexity of Read-Once Formulae
M. Mihail (Bellcore) :	On the Number of Eulerian Orientations of a Graph
B. Lhotzky (Bonn) :	An Approximation Algorithm for the Counting Problem for Multilinear Polynomials

THURSDAY, 13.6.1991

E. Upfal (IBM, San Jose) :	Computing with Noisy Information
T. Hagerup (Saarbrücken) :	On Parallel Counting
B. Schmeltz (Darmstadt) :	Lower Bounds on Probabilistic Circuits and Decision Trees
L. Kučera (Prague) :	Are there Difficult Coloring Problems?
T. Hofmeister (Dortmund) :	On the Complexity of Addition

Problem Session (Speakers: U. Vazirani, M. Karpinski, V. Vazirani, E. Upfal, A. Shamir, M. Santha)

FRIDAY, 14.6.1991

M. Karpinski (Bonn) :	Uniform Sampling Spaces for Approximate Counting in GF[q]
D.J.A. Welsh (Oxford) :	The Tutte Plane and FPRAS Problems
R. Rubinfeld (Princeton) :	Self-Testing / Correcting Programs
S. Kannan (Princeton) :	Checking the Correctness of Memories

O V E R V I E W

This Workshop was concerned with the newest development in the design of efficient (both sequential and parallel) randomized and pseudo-randomized algorithms as well as with the foundations of complexity theory of the randomized computation. The advantages of using randomization in the design of algorithms have been increasingly evident in the last couple of years. For some computational tasks it appears now that these algorithms are more efficient than the purely deterministic ones (in terms of the running time, hardware size, circuits depth, etc.). The very striking examples recently were the new randomized algorithms for enumerating the number of perfect matchings in certain classes of graphs or for some enumeration problems in the boolean algebra and finite fields. Solutions to these problems have applications ranging from the circuit design and coding theory to statistic mechanics and quantum field theory. The problem of deterministic simulation of certain classes of randomized algorithms and circuits was also another topic of this workshop.

The 34 participants of the workshop came from nine countries, eleven of them came from North America. The 24 lectures covered a wide body of research in *randomized algorithms.* Abstracts of the talks are listed in the next section.

The meeting was hold in a very informal and stimulating atmosphere. Thanks to everybody in Dagstuhl who made this workshop so interesting and enjoyable!

Acknowledgement. We are thankful to Angelika Mueller and Kathrin Schrader for their help in organizing this workshop.

Finding Hidden Hamiltonian Cycles

Andrei Broder
Digital Equipment Corporation
130 Lytton Ave., Palo Alto, CA 94301

Consider a random graph G composed of a Hamiltonian cycle on n labeled vertices and dn random edges that "hide" the cycle. Is it possible to unravel the structure, that is, to efficiently find a Hamiltonian cycle in G?

We describe an $O(n^3 \log n)$ steps algorithm A for this purpose, and prove that it succeeds almost surely. Part one of A properly covers the "trouble spots" of G by a collection of disjoint paths. (This is the hard part to analyze). Part two of A extends this cover to a full cycle by the rotation-extension technique which is already classical for such problems.

(Joint work with A. Frieze and Eli Shamir)

Random Walks on Unimodular Zonotopes

Martin Dyer
School of Computer Studies
University of Leeds
Leeds LS2 9JT

The rapid mixing of a random walk on the set of bases of a unimodular matrix is proved by associating it with a convex polyhedron; the zonotope, associated with the matrix. We also discuss an application to solving linear programs with totally unimodular constant systems in strongly polynomial tree via a variant of the simple method.

On Parallel Counting

Torben Hagerup
Max-Planck-Institut für Informatik
Im Stadtwald 15, 6600 Saarbrücken 11

We consider the parallel complexity of determining the number of 1's in a bit vector of length n. Wheras the exact problem cannot be solved in $o(\log n/ \log \log n)$ time with $n^{O(1)}$ processors, we show that an approximation of the number of 1's, correct up to a constant factor, can be computed in constant time on an n-processor concurrent-read concurrent-write PRAM with probability $1 - 2^{-n^{\Omega(1)}}$.

On the Complexity of Addition

Thomas Hofmeister
Lehrstuhl für Informatik
Universität Dortmund
Baroper Str. 301, 4600 Dortmund 50

In this talk, we see that the highest bit of addition, which is a monotone function, cannot be computed in polynomial-size, depth-2 threshold circuits which are monotone. This contrasts to a proof by Bruck who has shown that all bits of the addition can in fact be computed in poly-size, depth-2 general threshold circuits. Some other lower bounds which also hold for Bruck's circuits are only sketched.

Checking the Correctness of Memories

Sampath Kannan
Dept. of Computer Science
Princeton University
Princeton, NJ 08544

We extend the model of program checking to sequences of storage and retrieval operations. We show how a checker with $O(\log n)$-sized reliable memory can check that a memory of size n functions correctly with probability of success close to 1. We consider three memory organizations – queues, stacks, and RAMs.

We show lower bound on the size of reliable memory needed by the checker for two different cases. These lower bounds are tight.

Uniform Sampling Spaces for Approximate Counting $GF[q]$

Marek Karpinski
Dept. of Computer Science
Universität Bonn
Römerstr. 164, 5300 Bonn 1

We design the uniform sampling spaces for approximate counting the number of zeros and nonzeros of arbitrary polynomials $f(x_1, \ldots, x_n)$ over $GF[q]$, and design the first randomized polynomial time (ϵ, δ)-approximation algorithms for these problems. This gives the first efficient method for estimating the number of points on algebraic varieties over small finite fields other than $GF[2]$ (solved recently by Karpinski and Luby, *Proc. 2^{nd} ACM-SIAM SODA '91*), like $GF[3]$, the cases important for various approximation applications, e.g. in the circuit design, algebraic computation, and coding theory.

The algorithm is based on the sharp lower bound proved for the number of nonzeros of certain polynomials over $GF[q]$ in the function of the number of terms only. This could be also of independent algebraic or geometric interest.

We prove also a relative lower bound on the running time of an (ϵ, δ)-approximation algorithm for counting the number of zeros of polynomials, showing that any sublinear (in exponent) improvement on q would give subexponential randomized algorithm for 3SAT!

(joint work with D. Grigoriev)

Are there Difficult Coloring Problems?

Luděk Kučera
Dept. of Applied Mathematics
Charles University
Malostranské nám. 25, 11800 Prague 1, Czechoslovakia

A uniform Distribution over the class of k-colorable n-vertex graphs seems to yield a difficult coloring problem (w.r.t. average case time) - known polynomial time algorithms give unsatisfactory results if $k >> \sqrt{n}$ (while some of them perform a.s optimally for $k << \sqrt{n}$), the fastest a.s. optimal algorithm having complexity $n^{O(\log n)}$. Possible applications in cryptography were discussed.

An Approximation Algorithm for the Counting Problem for Multilinear Polynomials

Barbara Lhotzky
Dept. of Computer Science
Universität Bonn
Römerstr. 164, 5300 Bonn 1

The algebraic counting problem is defined as the problem of computing the number of solutions of polynomial equations $f(x_1, \ldots, x_n) = c$ over finite fields. The general algebraic counting problem is $\#P$-complete and there are only small classes of polynomials for which polynomial time counting algorithms are known. In this talk we present a randomized (ϵ, δ) approximation scheme computing, with high probability, a good estimation for the number of solution whose relative error is less than ϵ. The sequential running time of the algorithm is $O(nm^3qM(q)\frac{1}{\epsilon^2}ln\frac{1}{\delta})$ where n denote the number of variables, m the number of terms and q the order of the finite field. The time needed to multiply two elements of $GF[q]$ is denoted by $M(q)$. In the algorithm for counting the number of zeros of polynomials without constant terms, we can gain a factor m in running time.

(Joint work with M. Karpinski)

On Deterministic Approximation of DNF / Small Sample Spaces for Nonuniform Random Variables

Michael Luby
International Computer Science Institute
Berkeley, CA 94704

"The best throw of the die is to throw the die away" - Chinese fortune cookie

We develop efficient deterministic algorithms for approximating the fraction of truth assignments that satisfy a disjunctive normal form (DNF) formula. Let F be a DNF formula on n boolean variables with m clauses, and let u_F be the probability that a uniformly chosen truth assignment to the random variables satisfies F. For any constant ϵ, the algorithm on input ϵ and F produces an estimate Y that is within an additive factor ϵ of u_F. The running time of the algorithm is $(n+m)^{c \log\log(n+m)}$. Although the algorithm itself is deterministic, the analysis is probabilistic and uses the notion of limited independence between random variables.

(This is joint work with Boban Veličkovič)

Let $x_1, ..., x_n$ be binary valued random variables with specified probabilities $p_1, ..., p_n$, respectively, of being equal to 1. Our goal is to design a small efficiently constructible sample space that "approximates" the distribution where the variables are totally independent. We say that a distribution is a (k, ϵ) approximation if, for all k-tuples of the random variables and for all k-tuples of boolean values, the probability that the random variables are equal to the specified set of values is within ϵ of what it is when they are totally independent. Previous results consider the special case of the uniform distribution, i.e. all probabilities are one-half, and show how to construct a distribution that is a (k, ϵ) approximation with sample size $(\log n)^{2^{ck}}/\epsilon^c$ for a small constant c. We consider the general case when the specified probabilities are arbitrary and design a distribution that is a (k, ϵ) approximation with sample size essentially the same as for the uniform case. Our results extend in a straightforward way to the case when the variables are multi-valued and the probability for each variable for each value is arbitrary. An application of this work is to the problem of estimating the probability a DNF formula is satisfied when the boolean variables are chosen with nonuniform probabilities.

(This is joint work with Guy Even and Oded Goldreich)

Learning Decision Trees Using the Fourier Spectrum

Yishay Mansour
Aiken Computation Laboratory
Harvard University
Cambridge MA 02138

This work gives a polynomial time algorithm for learning decision trees with respect to the uniform distribution. The decision trees model that we consider is an extension of the traditional boolean decision trees model, and allows summation of a subset of the input over $GF[2]$ in each node.

We show how to learn in polynomial time any function that can be approximated (in norm L_2) by a polynomially sparse function. We demonstrate that any function whose sum of absolute value of the Fourier Transformation coefficients is polynomial can be approximated by a polynomially sparse function, and prove that boolean decision trees are in this class of functions.

On the Number of Eulerian Orientations of a Graph

Milena Mihail
Bell Communications Research
445 South Street, Morristown, NJ 07960

We give efficient randomized schemes to sample and approximately count Eulerian orientations of any Eulerian graph. Eulerian orientations are natural flow-like structures, and Welsh has pointed out that computing their number is equivalent to evaluating "ice-type partition functions" in statistical physics.

Our algorithms are based on a reduction to sampling and approximately counting perfect matchings for a class of graphs for which the methods of Broder, Jerrum and Sinclair, and others apply. A crucial step of the reduction is the "Monotonicity Lemma" which is of independent combinatorial interest. Roughly speaking, the Monotonicity Lemma establishes the intuitive fact that "increasing the number of constraints applied on a flow problem can only decrease the number of solutions". In turn, the proof of the lemma involves a new decomposition technique which decouples problematically overlapping structures (a recurrent obstacle in handling large combinatorial populations) and allows detailed enumeration arguments. As a byproduct, (i) we exhibit a class of graphs for which perfect and near-perfect matchings are polynomially related, and hence the permanent can be approximated, for reasons other than "short augmenting paths" (previously the only known approach); and (ii) we obtain a further direct sampling scheme for Eulerian orientations which is faster than the one suggested by the reduction to perfect matchings.

Finally, with respect to our approximate counting algorithm, we give complementary hardness result, namely, that counting exactly Eulerian orientations is $\#P$-complete, and provide some connections with Eulerian tours.

(Joint work with Peter Winkler)

Coloring Clique-Free Graphs in Linear Expected Time

Hans Jürgen Prömel
Forschungsinstitut für Diskrete Mathematik
Universität Bonn
Nassestr. 2, 5300 Bonn 1

In this talk we presented a linear expected time algorithm to color every graph which does not contain a clique on $l+1$ vertices as a subgraph with a minimal number of colors. This extends a result of Dyer and Frieze for l-colored graphs. For the proof we developed a new method which allows to precizely estimate the number of graphs with certain structured properties.

(Joint work with A. Steger)

Self-Testing/Correcting Programs

Ronitt Rubinfeld
Dept. of Computer Science
Princeton University
Princeton, NJ 08544

Suppose someone gives us an extremely fast program P that we can call as a black box to compute a function f. Should we trust that it works correctly? A *self-testing/correcting pair* for f allows us to: (1) estimate the probability that $P(x) \neq f(x)$ when x is randomly chosen; (2) on *any* input x, compute $f(x)$ correctly as long as P is not too faulty.

We present general techniques for constructing simple to program self-testing/correcting pairs for a variety of numerical functions.

(Part of the results in this talk are joint work with Manuel Blum and Mike Luby. The other results in this talk are joint work with Pete Gemmell, Dick Lipton, Madhu Sudan and Avi Wigderson.)

On the Monte Carlo Boolean Decision Tree Complexity of Read-Once Formulae

Miklos Santha
Laboratoire de Recherche en Informatique
BAT 490, 91405 Orsay

In the boolean decision tree model there is at least a linear gap between the Monte Carlo and the Las Vegas complexity of a function depending on the error probability. We prove for a large class of read-once formulae that this trivial speed-up is the best what a Monte Carlo algorithm can achieve. 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. The result follows from a general lower bound that we derive on the Monte Carlo complexity of these formulae. This bound is analogous to the lower bound obtained by Saks and Wigderson on their Las Vegas complexity.

Lower Bounds on Probabilistic Circuits and Decision Trees

Bernd Schmeltz
Institut für Theoretische Informatik
Technische Universität Darmstadt
Alexanderstr. 10, 6100 Darmstadt

A noisy circuit is one where the output of each gate is flipped with probability (at most) ϵ. A noisy decision tree is one where each query is answered incorrectly with probability ϵ. We distinguish between static decision trees (where each computation path contains the same queries) and dynamic ones.

Noisy circuits (static decision trees) are shown to require size (depth) $\Omega(s \log s)$ in order to compute a function with sensitivity s reliably. We also give a condition for boolean functions which forces a noisy dynamic decision tree to have depth $\Omega(n \log n)$. This condition is satisfied by almost all boolean functions.

Let $U^{(0)}$ ($U^{(1)}$) be a vector of random variables the values of which determine the output of the decision tree. To satisfy the confidence parameter δ

$$\sum_{n} |Pr(U^{(0)} = u) - Pr(U^{(1)} = u)| \geq 2 - 4\delta$$

must be satisfied. (The sum ranges over all possible values of the random variables.) Calculating the left hand side of the inequality establishes the lower bound.

An Efficient Cryptographic Hash Function

Claus P. Schnorr
FB Informatik
Universität Frankfurt
6000 Frankfurt am Main 1

We propose an efficient algorithm that hashes messages of arbitrary bit length into 128 bit hash value. The algorithm is designed to make the production of a pair of colliding messages computationally infeasible. The algorithm has interesting provable properties. Each hash value in $\{0,1\}^{128}$ occurs with frequency at most 2^{-120}.

Analysis of Multi Prover Protocols

Adi Shamir
Applied Math. Dept.
Weizmann Institute of Science
Rehovot 76100

The model of multi-prover interactive proofs was introduced several years ago by Ben-Or, Goldwasser, Kilian and Wigderson. A major open problem is whether the parallel execution of n copies of such proofs reduces the probability of cheating exponentially fast in n. In this talk we show that this is indeed the case in NP-protocols, but that the probability of cheating is only bounded by $2^{-\frac{n}{9}}$ rather than the expected 2^{-n}.

(Joint work with Dror Lapidot)

The Kleitman-Rothschild Method and an Application to Perfect Graphs

Angelika Steger
Forschungsinstitut für Diskrete Mathematik
Universität Bonn
Nassestr. 2, 5300 Bonn 1

In 1975 Kleitman and Rothschild proved an asymptotic formula for the number of partial orders of an n-element set. In this talk we extend their ideas to a general method which provides a framework for showing that two sets of graphs are asymptotically equal. In the second part of the talk we combine this method with Szemerédi's uniformity Lemma to prove an asymptotic version of a long standing conjecture in perfect graph theory:
Let *Perf*(n) denote the set of all perfect graphs on n vertices and let *Berge*(n) denote the set of all Berge graphs on n vertices. The strong perfect graph conjecture states that $Perf(n) = Berge(n)$. We prove that this conjecture is at least asymptotically true i.e. we show $\lim_{n\to\infty} \frac{|Perf(n)|}{|Berge(n)|} = 1$.

(These results were obtained jointly with H. J. Prömel)

Randomized On-Line Coloring has Performance Ratio $\frac{n}{\log^2 n}$

Mario Szegedy
Dept. of Computer Science
University of Chicago
Chicago, IL 60637

Performance ratio of algorithm A = # of colors A uses / chromatic number of G (for the worst G). Lovász, Trotter, Saks prove:

There is a deterministic on-line coloring algorithm that has performance ratio $n/\log^* n$.

Wishvanathan has found a randomized on-line coloring algorithm with performance ratio $n/\log n$.
We prove the following lower bounds:

i) in the deterministic case no algorithm (on-line) can perform better than $n/\log^2 n$.

ii) in the randomized case no on-line algorithm performs better than $n/log^3 n$.

Computing with Noisy Information

Eli Upfal
IBM Almaden Research Center
650 Harry Road, San Jose, CA 95193

This talk studies the depth of *noisy* decision trees in which each node gives the wrong answer with some constant probability. In the *noisy boolean decision tree* model we give tight bounds on the number of queries to input variables required to compute threshold functions, the parity function and symmetric functions. In the *noisy comparison tree* model we give tight bounds on the number of noisy comparisons for sorting, selection and merging. We also study parallel selection and sorting with noisy comparisons, giving tight bounds for several problems.

(Joint work with Uriel Feige, David Peleg, and Prabhakar Raghavan)

A Subexponential Algorithm for Approximating the Permanent

Umesh Vazirani
Computer Science Division
University of California, Berkeley
Berkeley, CA 94720

Computing 0/1 permanents (the number of perfect matchings in a bipartite graph) is a fundamental problem in combinatorics. The previous best approximation algorithm for this problem due to Karmarkar, et al. had a running time of $O(2^{n/2})$. We give a new algorithm with a running time of $2^{\tilde{O}(\sqrt{n})}$. Our algorithm is based on the Markov chain algorithm of Jerrum & Sinclair.

(Joint work with Mark Jerrum)

Fast Parallel Algorithms for Matroid Union, Arboresences, and Edge-Disjoint Spanning Trees

Vijay V. Vazirani
Dept. of Computer Science & Engineering
Indian Institute of Technology
New Delhi 110016

We give an RNC algorithm for finding a maximum independent set in the union of matroids $M_1, M_2, \dots, M_k$ which are specified by their linear representations over Q. This yields RNC algorithms for the classical problems of matroid covering and packing. For the special case of graphic matroids, these problems correspond respectively to finding an arboresence in the given graph (*i.e.* a minimum number of forests that cover all the edges), and finding a largest set of edge-disjoint spanning trees in it. Our algorithms have two main ingredients: a simple method for obtaining a representation for the union matroid via randomization, and the Isolating Lemma of Mulmuley/Vazirani/Vazirani.

(Joint work with H. Narayanan and H. Saran)

The Tutte Plane and FPRAS Problem

Dominic J. A. Welsh
Mathematical Institute
Merton College
24 St. Giles, Oxford

I extend the theorem of M. Mihail and P. Winkler given earlier this week by showing.

Theorem 1. *Exact counting of Eulerian orientations on a 4-regular planar graph is #P-complete.*

The proof of this leads to

Theorem 2. *There exist FPRAS for evaluating the Tutte polynomial of a plane graph at all points of the form*

$$\begin{array}{l} (3^k\ ,\ 1+\dfrac{4}{3^k-1}) \\ (1+\dfrac{4}{3^k-1}\ ,\ 3^k) \end{array} \qquad k=1,2,\ldots$$

Note all these points lie on the hyperbole $H_4 \equiv (x-1)(y-1) = 4$ which corresponds to the 4-state Potts model of statistical physics. These are the first points outside the Ising hyperbole H_2 which are #P-hard to evaluate but have a FPRAS.

Simulating BPP Using a General Weak Random Source

David Zuckerman
Computer Science Division
University of California
Berkeley, CA 94720

We show how to simulate BPP and approximation algorithms in polynomial time using the output from a δ-source. A δ-source is a weak random source that is asked only once for R bits, and must output an R-bit string according to some distribution that places probability no more than $2^{-\delta R}$ on any particular string. We also present applications to the problem of implicit $O(1)$ probe search and to showing the difficulty of approximating MAX CLIQUE.

Participants:

Helmut **Alt**
Institut für Informatik
Freie Universität Berlin
Arnimallee 2-6
1000 Berlin 33
alt@tcs.fu-berlin.de

Andrei **Broder**
Digital Equipment Corporation
130 Lytton Ave
Palo Alto, CA 94301
USA
broder@src.dec.com

M. **Dietzfelbinger**
Fachbereich Informatik
Universität Paderborn
W-4790 Paderborn

Martin **Dyer**
School of Computer Studies
University of Leeds
Leeds LS2 9JT
United Kingdom
dyer@dcs.leeds.ac.uk

Torben **Hagerup**
Max-Planck-Institut für Informatik
Im Stadtwald 15
W-6600 Saarbrücken 11
torben@cs.uni-sb.de

Thomas **Hofmeister**
Lehrstuhl für Informatik II
Universität Dortmund
Baroperstr. 301
W-4600 Dortmund 50
hofmeister@zorro.informatik.uni-dortmund.de

Sampath **Kannan**
University of Arizona
Dept. of Computer Science
Gould-Simpson 721
Tucson, AZ 85721
USA
kannan@cs.arizona.edu

M. **Karonski**
Dept. of Mathematics
Adam Mickiewicz University
Poznan
POLEN
karonski@pluam11.bitnet

Marek **Karpinski**
Institut für Informatik
Universität Bonn
W-5300 Bonn 1
marek@cs.uni-bonn.de

Ludek **Kucera**
Dept. of Applied Mathematics
Charles University
Malostranské nám 25
11800 Prague 1
Czechoslovakia
UMALK@CSEARN.bitnet

Barbara **Lhotzky**
Dipl. Inform.
Institut für Informatik V
Universität Bonn
W-5300 Bonn 1
lhotzky@cs.bonn.edu

M. **Luby**
International Computer Science Institute
Berkeley, CA 94704
USA
luby@icsib9.berkeley.edu

Y. **Mansour**
Aiken Computation Laboratory
Harvard University
Cambridge MA 02138
USA
mansour@harvard.edu

Kurt **Mehlhorn**
Max Planck-Institut für Informatik
Im Stadtwald 15
W-6600 Saarbrücken 11
mehlhorn@cs.uni-sb.de

Milena **Mihail**
2M-354, Bellcore
445 South Street
Morristown, NJ 07960
USA
mihail@bellcore.com

H.-J. **Prömel**
Forschungsinstitut für Discrete Mathematik
Universität Bonn
Nassestr. 2
W-5300 Bonn 1
proemel@dbnuor1.bitnet

Rüdiger **Reischuk**
Institut für Theoretische Informatik
TH Darmstadt
W-6100 Darmstadt

Ronitt **Rubinfeld**
Dept. of Computer Science
Princeton University
Princeton, NJ 08544
USA
rr@elan.princeton.edu

Miklos **Santha**
Laboratoire de Recherche en Informatique
BAT 490
91405 Orsay
France
santha@lri.lri.fr

Bernd **Schmeltz**
Dipl. Math.
Institut für Theoretische Informatik
Technische Universität Darmstadt
Alexanderstr. 10
W-6100 Darmstadt
XITIBSCH@DDATHD21

C.P. **Schnorr**
FB Informatik
Universität Frankfurt
PSF 11932
W-6000 Frankfurt am Main 1
schnorr@informatik.uni-frankfurt.de

A. **Shamir**
Applied Math. Dept.
Weizmann Institute of Science
Rehovot 76100
Israel
shamir@wisdom.bitnet

Angelika **Steger**
Forschungsinstitut für Diskrete Mathematik
Universität Bonn
Nassestraße 2
W-5300 Bonn 1
or210@dbnuor1

Mario **Szegedy**
Dept. of Computer Science
University of Chicago
Chicago, IL 60637
USA
mario@tartarus.uchicago.edu

Ely **Upfal**
Dept. K 53
IBM Almaden Research Center
650 Harry Road

San Jose, CA 95193
USA
ely@ibm.com

Umesh **Vazirani**
Computer Science Division
University of California, Berkeley
Berkeley, CA 94720
USA
vazirani@vina.berkeley.edu

Vijay V. **Vazirani**
Dept. of Computer Science & Engineering
Indian Institute of Technology
New Delhi 110016
India
vazirani@netearth.ernet.in

Boban **Velickovic**
Mathematics Department
University of California, Berkeley
Berkeley, CA 94720
USA
velickov@math.berkeley.edu

Dominic J.A. **Welsh**
Merton College
Oxford
Great Britain

Thorsten **Werther**
Institut für Informatik
Universität Bonn, Abt. V
Römerstraße 164
W-5300 Bonn 1
werther@cs.bonn.edu

Thomas **Zeugmann**
Institut für Theoretische Informatik
Technische Universität Darmstadt
Alexanderstr. 10
W-6100 Darmstadt
xititzeu@ddathd21.bitnet

David **Zuckerman**
Computer Science Division
University of California
Berkeley, CA 94720
USA
diz@harmony.berkeley.edu /
diz@theory.lcs.mit.edu

Bisher erschienene und geplante Titel:

W. Gentzsch, W.J. Paul (editors):
Architecture and Performance, Dagstuhl-Seminar-Report; 1, 18.-20.6.1990; (9025)

K. Harbusch, W. Wahlster (editors):
Tree Adjoining Grammars, 1st. International Worshop on TAGs: Formal Theory and Application, Dagstuhl-Seminar-Report; 2, 15.-17.8.1990 (9033)

Ch. Hankin, R. Wilhelm (editors):
Functional Languages: Optimization for Parallelism, Dagstuhl-Seminar-Report; 3, 3.-7.9.1990 (9036)

H. Alt, E. Welzl (editors):
Algorithmic Geometry, Dagstuhl-Seminar-Report; 4, 8.-12.10.1990 (9041)

J. Berstel , J.E. Pin, W. Thomas (editors):
Automata Theory and Applications in Logic and Complexity, Dagstuhl-Seminar-Report; 5, 14.-18.1.1991 (9103)

B. Becker, Ch. Meinel (editors):
Entwerfen, Prüfen, Testen, Dagstuhl-Seminar-Report; 6, 18.-22.2.1991 (9108)

J. P. Finance, S. Jähnichen, J. Loeckx, M. Wirsing (editors):
Logical Theory for Program Construction, Dagstuhl-Seminar-Report; 7, 25.2.-1.3.1991 (9109)

E. W. Mayr, F. Meyer auf der Heide (editors):
Parallel and Distributed Algorithms, Dagstuhl-Seminar-Report; 8, 4.-8.3.1991 (9110)

M. Broy, P. Deussen, E.-R. Olderog, W.P. de Roever (editors):
Concurrent Systems: Semantics, Specification, and Synthesis, Dagstuhl-Seminar-Report; 9, 11.-15.3.1991 (9111)

K. Apt, K. Indermark, M. Rodriguez-Artalejo (editors):
Integration of Functional and Logic Programming, Dagstuhl-Seminar-Report; 10, 18.-22.3.1991 (9112)

E. Novak, J. Traub, H. Wozniakowski (editors):
Algorithms and Complexity for Continuous Problems, Dagstuhl-Seminar-Report; 11, 15-19.4.1991 (9116)

B. Nebel, C. Peltason, K. v. Luck (editors):
Terminological Logics, Dagstuhl-Seminar-Report; 12, 6.5.-18.5.1991 (9119)

R. Giegerich, S. Graham (editors):
Code Generation - Concepts, Tools, Techniques, Dagstuhl-Seminar-Report; 13, , 20.-24.5.1991 (9121)

M. Karpinski, M. Luby, U. Vazirani (editors):
Randomized Algorithms, Dagstuhl-Seminar-Report; 14, 10.-14.6.1991 (9124)

J. Ch. Freytag, D. Maier, G. Vossen (editors):
Query Processing in Object-Oriented, Complex Object, and Nested Relation Databases, Dagstuhl-Seminar-Report; 15, 17.-21.6.1991 (9125)

M. Droste, Y. Gurevich (editors):
Semantics of Programming Languages and Model Theory, Dagstuhl-Seminar-Report; 16, 24.-28.6.1991 (9126)