Report No. 8515 - CS

BONN WORKSHOP ON

FOUNDATIONS OF COMPUTING

BONN, JUNE 28 - JULY 3, 1987

BFC 87

with two special programs on

- RANDOMISED AND PARALLEL COMPUTATION
- COMPLEXITY OF COMPUTATION IN ALGEBRA, GEOMETRY, AND NUMBER THEORY

PROGRAM CO-CHAIRMEN:

MAREK KARPINSKI AND VOLKER STRASSEN

Max-Planck-Institut für Mathematik, Bonn
Department of Computer Science, University of Bonn

Bonn Workshop on Foundations of Computing
Bonn, June 28 - July 3, 1987

Organized by:

Max-Planck-Institut für Mathematik, Bonn
Department of Computer Science,
University of Bonn

Supported by:

Deutsche Forschungsgemeinschaft,
Bonn-Bad Godesberg

Sponsors:

Addison-Wesley Bonn
Apple Computer GmbH München
Buchhandlung Behrendt Bonn
Compaq Computer GmbH München
Daimler-Benz AG Stuttgart
Digital Equipment GmbH Köln
Gerling-Konzern Köln
IBM Deutschland GmbH Stuttgart
Lufthansa AG Köln
Siemens AG München

Program Secretary and Organization: Mariele Knepper

Layout: Susanne Sollmann

Program Committee:

Ravi Kannan,
Marek Karpinski, co-chairman
László Lovász,
Hendrik W. Lenstra Jr.,
Michael Sipser,
Volker Strassen, co-chairman
Eli Upfal,
Don Zagier

Contents:

List of Participants

Program of the Workshop

Abstracts of the Program Lectures:

László Babai, *Parallel Algorithms for Permutation Groups*

Shafi Goldwasser, *How to Certify Primes Quickly Using Elliptic Curves*

Johan Hastad, *Lower Bounds for Small Depth Circuits*

Erich Kaltofen, *Randomized Parallel Computation of Matrix Canonical Forms*

Richard M. Karp, *Complexity of Parallel Computation*

Marek Karpinski, *Multigrade Forms and Circuit Complexity of Bipartite Matching*

Hendrik W. Lenstra Jr., *Elliptic Curves and Algorithms*

László Lovász, *Algorithmic Problems in Geometry*

Kurt Mehlhorn, *Homotopic River Routing*

Andrew Odlyzko, *On Riemann's Zeta Function*

Michael O. Rabin, *Randomized Computation*

Claus-Peter Schnorr, *The Multiplicative Complexity of Pairs of Quadratic Boolean Forms*

Arnold Schönhage, *GCD Computations*

Eli Shamir, *Subdominant Eigenvalues for Random d-Graphs*

Volker Strassen, *Complexity of Bilinear Problems*

Eli Upfal, *Finding Disjoint Paths on Expanders Graphs*

Umesh V. Vazirani, *Asymmetry and Efficient Randomized Computation*

Avi Wigderson, *Lower Bounds on Parallel RAMs*

Don Zagier, *Introduction to Elliptic Curves*

Abstracts of the Technical Sessions:

Noga Alon, *Tight Bounds for the Complexity of Randomised Comparison Sorting Algorithms*

Wieb Bosma, *New Techniques in Primality Testing*

Gilles Brassard, *Minimum Information Proofs of Knowledge*

Andrea Clivio, *The Complexity of Tiling Rectangles with Rectangles*

Henri Cohen, *Atkin's Primality Test*

Elias Dahlhaus, *Parallel Algorithms on Chordal Graphs*

Martin Fürer, *Universal Hashing in VLSI*

Susan Landau, *Polynomial Decomposition Algorithms*

R. Mirwald, *The Multiplicative Complexity of Single Quadratic Boolean Forms*

Rüdiger Reischuk, *Probabilistic Communication*

Prasoon Tiwari, *A Deterministic Algorithm for Sparse Multivariate Polynomial Interpolation*

Rutger Verbeek, *Separating Randomised Complexity Classes*

Manfred Warmuth, *Expected Mistake Bounds for On-Line Learning Algorithms*

List of Participants:

N. Alon, Tel Aviv
T. Althans, Bonn
M. D. Atkinson, Ottawa
L. Babai, Budapest
L. Balke, Bonn
M. Bardey, Bonn
J. Bar-Ilan, Jerusalem
A. Bar-Noy, Jerusalem
M. Betke, Bonn
K.-H. Boehling, Bonn
W. Bosma, Amsterdam
G. Brassard, Amsterdam
B. von Braunmühl, Bonn
A. Broder, Palo Alto
A. Brück, Köln
Brustmann, Frankfurt
J. Buchmann, Düsseldorf
P. Burgisser, Uni Zürich
C. Busch, Bonn
A. Clivio, ETH Zürich
A. Cohen, Jerusalem
H. Cohen, Bordeaux
C. Crepeau, MIT
E. Dahlhaus, Bonn
F. De La Wega, Paris Sud
G. Dueck, IBM Heidelberg
C. Eckhardt, Göttingen
K. Elles, Bonn
P. van Emde Boas, Amsterdam
V. Ernst, Wermelskirchen
U. Esser, Köln
T. Fabian, Bonn
F. E. Fich, Toronto
D. Ford, Montreal
T. Fox, Solingen
R. Franke, Bonn
E. Fuß, Bonn
M. Fürer, Uni Zürich
S. Gao, Saarbrücken
K. Geisen, Bonn
R. Gengler, Bonn
M. Gergeleit, Bonn
Gil, Jerusalem
C. Gladenbeck, Bonn

S. Goldwasser, MIT
W. Gorzalka, Bonn
E. Grädel, Basel
F. Grunewald, Bonn
T. Hagerup, Saarbrücken
J. Hastad, MIT
F. Hirzebruch, Bonn
A. Hoene, TU Berlin
R. Hofestädt, Bonn
A. Hopp, Bonn
M.-P. van der Hulst, Amsterdam
R. Janßen, Heidelberg
M. Jaxi, GMD
B. Just, Frankfurt
D. Kaese, Bonn
E. Kaltofen, Troy
R. Kannan, Bonn
M. Karchmer, Jerusalem
R. M. Karp, Berkeley
M. Karpinski, Bonn
M. Kaufmann, Saarbrücken
H. Kleisli, Fribourg
N. Konalewski, Bonn
M. Kummer, Karlsruhe
M. Kunde, TU München
S. Landau, Wesleyan
M. Lange, Frankfurt
G. von Laszewski, Bonn
C. Lautemann, Bremen
H. Lefmann, Bielefeld
H. W. Lenstra, Berkeley
K. Lenz, Frankfurt
B. Lhotzky, Bonn
T. Lickteig, Uni Zürich
J. van der Lingen, Amsterdam
L. Lovász, Budapest
P. A. Matthews, Aarhus
K. Mehlhorn, Saarbrücken
H. Meier, Bonn
U. Meyer, Bonn
P. Mihailescu, ETH Zürich
R. Mirwald, Frankfurt
A. Möbus, Düsseldorf
K. Möller, Bonn
T. Mossakowski, Bremen

S. Naor, Jerusalem
A. Odlyzko, Murray Hill
C. A. Petri, GMD
M. O. Rabin, Harvard
R. Reischuk, Darmstadt
J. E. Riedel, Bonn
R. Rodriguez, GMD
C. Rüb, Saarbrücken
M. Santha, Paris Sud
I. Schiermeyer, Aachen
J. Schietke, Bonn
D. Schmidt, Köln
M. Schmidt, Solingen
C.-P. Schnorr, Frankfurt
A. Schönhage, Tübingen
U. Schöning, Koblenz
P. Schüller, Bonn
H. Seidel, Frankfurt
E. Shamir, Jerusalem
N. Shavit, Jerusalem
H.-U. Simon, Saarbrücken
U. Steinhausen, Bonn
C. Storb, Saarbrücken
V. Strassen, Uni Zürich
W. Strokosch, Bonn
R. M. Tan, Utrecht
P. Tiwari, IBM Yorktown Heights
V. Tobler, Uni Zürich
C. Traverso, Pisa
E. Upfal, IBM San Jose
U. V. Vazirani, Harvard
V. V. Vazirani, Murray Hill
A. van der Vekens, Bonn
M. Veldhorst, Utrecht
R. Verbeek, Bonn
D. Wagner, Aachen
F. Wagner, Aachen
H. Wagner, Dortmund
K. Wagner, Augsburg
M. Warmuth, Santa Cruz
I. Wegener, Frankfurt
W. Welke, Bonn
B. Werther, Bonn
K. Werther, Bonn
T. Werther, Bonn

A. Wigderson, Jerusalem

F. Wille, Köln

C. Williamson, Univ. of Cal.

D. Zagier, Bonn

SUNDAY, JUNE 28

13.00-18.00 Registration
(University Building, Wegelerstrasse 10)

20.00 Reception

MONDAY, JUNE 29

9.00 Opening

Morning Session:

9.15 Michael O. Rabin (Harvard)
Randomised Computations I

10.15 Michael O. Rabin (Harvard)
Randomised Computations II

11.15 László Babai (Budapest)
Parallel Algorithms for Permutation Groups

Afternoon Session:

15.00 Don Zagier (Bonn)
Introduction to Elliptic Curves I

16.00 Don Zagier (Bonn)
Introduction to Elliptic Curves II

17.00 Shafi Goldwasser (MIT)
How to Certify Primes Quickly Using Elliptic Curves

18.00 Claus-Peter Schnorr (Frankfurt)
The Multiplicative Complexity of Pairs of Quadratic Boolean Forms

20.15 Evening Sessions on Elliptic Curves, Primality Tests and Cryptography

TUESDAY, JUNE 30

Morning Session:

9.45 Michael O. Rabin (Harvard)
Randomised Computations III

10.45 Erich Kaltofen (Troy)
Randomised Parallel Computation of Matrix Canonical Forms

11.45 Hendrik W. Lenstra Jr. (Berkeley)
Elliptic Curves and Algorithms I

12.45 Andrew Odlyzko (Murray Hill)
On Riemann's Zeta Functions I

Afternoon Session:

15.00 Arnold Schönhage (Tübingen)
GCD Computations

16.00 Eli Shamir (Jerusalem)
Subdominant Eigenvalues For Random d-Graphs

17.00 Eli Upfal (IBM San Jose)
Finding Disjoint Paths on Expanders Graphs

20.15 Evening Sessions on Complexity of Computation in Algebra and Geometry of Numbers

WEDNESDAY, JULY 1

Morning Session:

9.15 Hendrik W. Lenstra Jr. (Berkeley)
Elliptic Curves and Algorithms II

10.15 Hendrik W. Lenstra Jr. (Berkeley)
Elliptic Curves and Algorithms III

11.15 Andrew Odlyzko (Murray Hill)
On Riemann's Zeta Functions II

12.15 Andrew Odlyzko (Murray Hill)
On Riemann's Zeta Functions III

Wednesday Afternoon:

15.00 Rhine Boat Excursion

THURSDAY, JULY 2

Morning Session:

9.45 Richard M. Karp (Berkeley)
Complexity of Parallel Computation I

10.45 Richard M. Karp (Berkeley)
Complexity of Parallel Computation II

11.45 László Lovász (Budapest)
Algorithmic Problems in Geometry I

12.45 László Lovász (Budapest)
Algorithmic Problems in Geometry II

Afternoon Session:

15.00 Volker Strassen (Zürich)
Complexity of Bilinear Problems I

16.00 Volker Strassen (Zürich)
Complexity of Bilinear Problems II

17.00 Kurt Mehlhorn (Saarbrücken)
Homotopic River Routing

20.15 Evening Sessions on Randomised and Parallel Computation

FRIDAY, JULY 3

Morning Session:

9.15 Richard M. Karp (Berkeley)
Complexity of Parallel Computation III

10.15 Richard M. Karp (Berkeley)
Complexity of Parallel Computation IV

11.15 László Lovász (Budapest)
Algorithmic Problems in Geometry III

12.15 Volker Strassen (Zürich)
Complexity of Bilinear Problems III

Afternoon Session:

15.00 Johan Hastad (MIT)
Lower Bounds for Small Depth Circuits

16.00 Marek Karpinski (Bonn)
Multigrade Forms and Circuit Complexity of Bipartite Matching

17.00 Umesh Vazirani (Harvard)
Asymmetry and Efficient Randomized Computation

18.00 Avi Wigderson (Jerusalem)
Lower Bounds on Parallel RAMs

□

PROBLEM SESSIONS

Problem Sessions Scheduled:

1. Complexity of Parallel Computation
2. Randomised Parallel Algorithms
3. VLSI Algorithms and Architectures
4. Lower Bounds for the Circuit Complexity
5. Complexity of Computation in Algebra
6. Algorithms and the Geometry of Numbers
7. Elliptic Curves, Primality Tests and Cryptography

These were divided into three Evening Sessions on

- Elliptic Curves, Primality Tests and Cryptography (Session 7; Chair: Hendrik W. Lenstra and Don Zagier)
- Complexity of Computation in Algebra and Geometry of Numbers (Sessions 5 and 6; Chair: Ravi Kannan and Volker Strassen)
- Randomised and Parallel Computation (Sessions 1-4; Chair: Marek Karpinski and Eli Upfal)

Participants in the Problem Sessions:

N. Alon (Tel Aviv)
Tight Bounds for the Complexity of Randomised Comparison Sorting Algorithms

W. Bosma (Amsterdam)
New Techniques in Primality Testing

G. Brassard (Amsterdam)
Minimum Information Proofs of Knowledge

A. Clivio (Zürich)
The Complexity of Tiling Rectangles with Rectangles

H. Cohen (Bordeaux)
Atkin's Primality Test

E. Dahlhaus (Bonn)
Parallel Algorithms on Chordal Graphs

M. Fürer (Zürich)
Universal Hashing in VLSI

S. Landau (Wesleyan)
Polynomial Decomposition Algorithms

R. Mirwald (Frankfurt)
The Multiplicative Complexity of Single Quadratic Boolean Forms

R. Reischuk (Darmstadt)
Probabilistic Communication

P. Tiwari (IBM Yorktown Heights)
A Deterministic Algorithm for Sparse Multivariate Polynomial Interpolation

R. Verbeek (Bonn)
Separating Randomised Complexity Classes

M. Warmuth (Santa Cruz)
Expected Mistake Bounds for On-Line Learning Algorithms

□

Program Lectures

TITLE: Permutation Groups in NC

AUTHOR: *László Babai* *

AFFILIATION: Eötvös University, Budapest, and University of Chicago

Abstract

We show that the basic problems of permutation group manipulation admit efficient parallel solutions. Given a permutation group G by a list of generators, we find a set of NC-efficient strong generators in NC. Using this, we show, that the following problems are in NC: membership in G; determining the order of G; finding the center of G; finding a composition series of G along with permutation representations of each composition factor. Moreover, given G, we are able to find the pointwise stabilizer of a set in NC. One consequence is that isomorphism of graphs with bounded multiplicity of eigenvalues is in NC.

The analysis of the algorithms depends, in several ways, on consequences of the classification of finite simple groups.

Co-authors:

Eugene M. Luks †
University of Oregon

Ákos Seress *
Mathematical Institute of the Hungarian Academy of Sciences

TITLE: Certifying Primes Quickly

AUTHOR: Shafi Goldwasser (Joint with Joe Kilian)

AFFILIATION: MIT

We presented a probabilistic primality test which outputs short proofs of its assertions of primality.

The algorithm terminates in expected polynomial time on all but at most $O\left(\frac{1}{2^{k^{\varepsilon}}}\right)$ OF THE K-BIT PRIMES.

UNDER plausible condition on the distribution of primes in small intervals, the algorithm runs in expected polynomial time on all primes.

The algorithm uses techniques from the theory of elliptic curves.

Finally, a general condition on families of groups which can be used for primality testing, was developed.

TITLE: LOWER BOUNDS FOR SMALL-DEPTH CIRCUITS

AUTHOR: JOHAN HASTAD

AFFILIATION: MIT

We consider the model of small-depth circuits, i.e. circuits containing AND-gates, OR-gates and negations where the distance from any input to the output is small (e.g. constant or growing very slowly with the input length).

We prove the following results.

1: If the depth is restricted to k, parity require circuits of size $\exp(cn^{\frac{1}{k-1}})$.

2: Polynomial size circuits computing parity require depth $\frac{\log n}{\log\log n} - c\frac{\log n}{(\log\log n)^2}$ for some constant c.

3. There are functions f_k which can be computed by linear size circuits of depth k but require circuits of size $\exp(-cn^{\frac{1}{2k}}/\log n)$.

TITLE: LOWER BOUNDS FOR SMALL-DEPTH CIRCUITS

AUTHOR: JOHAN HASTAD

AFFILIATION: MIT

The key method is the use of random restrictions as introduced by Furst, Saxe and Sipser.

As was previously known these results imply that there is an oracle B such that

$$PSPACE^B \neq PH^B \quad \text{and} \quad \Sigma_i^B \neq \Sigma_{i+1}^B .$$

Here PH denotes the polynomial time hierarchy and Σ_i are the levels within the polynomial time hierarchy.

TITLE: Randomized parallel computation of matrix canonical forms

AUTHOR: Erich Kaltofen

AFFILIATION: Rensselaer Polytechnic Institute

Joint work with M.S. Krishnamoorthy (RPI) and B. D. Saunders (Univ Delaware)

Fast parallel (poly-log depth with polynomially many processors) algorithms are discussed for matrices with polynomial entries over a field. We give an NC^2 solution for simplification to Hermite normal form and thus can find the polynomial solution of linear systems in NC^2. Furthermore, a parallel Las-Vegas randomized algorithm to construct the Smith normal form of a polynomial matrix together with transforming unimodular multipliers is discussed. Applications include the RNC^2 construction of the Frobenius form of a matrix with

TITLE:

AUTHOR:

AFFILIATION:

entries from a field and an RNC^3 of the block structure of the Jordan normal form.

TITLE: Complexity of Parallel Computation

AUTHOR: Richard M. Karp

AFFILIATION: University of California at Berkeley

These lectures are concerned with the complexity of solving computational problems on shared-memory parallel random-access machines. The fundamental resources considered are the computation time $T(n)$ and the number of processors $P(n)$. A parallel algorithm is considered efficient if the product $T(n)P(n)$ is not much greater than the best possible sequential execution time. We give efficient parallel algorithms for several problems about data structures, graphs, sorting and algebraic expressions. Then we introduce N.C, the class of problems solvable with $T(n) = O(\log^k n)$ and $P(n) = O(n^c)$. We show that the problems of inverting a matrix or computing its rank are in NC. Finally we discuss P-complete problems; these are solvable sequentially in polynomial time, but are unlikely to lie in NC.

TITLE: Multigrade Forms and Circuit Complexity of Bipartite Matching

AUTHOR: Marek Karpinski

AFFILIATION: University of Bonn

We prove that the problem of deciding and constructing a perfect matching in bipartite graphs G with the polynomial permanents of their $n \times n$ adjacency matrices A ($perm(A) = n^{O(1)}$) are in parallel deterministic classes NC^2, and NC^3, respectively. We further design an NC^3 algorithm for the problem of constructing all perfect matchings (enumerator problem) in a graph with a permanent bounded by $O(n^k)$. The basic steps were the development of a new symmetric functions method for the decision algorithm, and the new parallel technique for the matching enumerator problem. The enumerator-algorithm works in $O(\log^3 n)$ parallel time, and $O(n^{3k+5.5} \cdot \log n)$ processors. Due to this algorithm, the problems of Maximum Weighted Matching (weights in binary), First Lexicographical Perfect Matching, and the Stable Marriage Problems are all in NC^3, provided

TITLE:

AUTHOR: Karpinski

AFFILIATION:

the number of underlying matchings is 'small'. Also, as a consequence of the enumerator, inherently difficult problems of counting 'perm(A) mod k' have been proved efficiently parallelisable for the polynomially small permanents.

Concerning the circuit complexity of the logical permanent, we display classes of bounded permanents problems, each of superpolynomial monotone circuit complexity ($n^{\Omega(\log n)}$) which are computable within the uniform NC^2. We connect this with some complexity problems of integer multigrade forms stemming from our symmetric functions method for the logical permanent. (joint work with D.Y. Grigoriev)

□

TITLE: P-ADIC FACTORIZATION AND FINDING MAXIMAL ORDERS

AUTHOR: H.W. LENSTRA, JR.

AFFILIATION: MATH.
UNIV. OF CALIFORNIA
BERKELEY

THE FOLLOWING TWO PROBLEMS ARE CONSIDERED.

1. (P-ADIC FACTORIZATION) LET A PRIME NUMBER p BE GIVEN, AND A MONIC POLYNOMIAL $f \in \mathbb{Z}[X]$. SUPPOSE THAT $f = \prod f_i$ IS THE FACTORIZATION OF f INTO IRREDUCIBLES IN $\mathbb{Z}_p[X]$, WHERE $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ IS THE RING OF p-ADIC INTEGERS. PROBLEM: DETERMINE THE $f_i \bmod p^m \in (\mathbb{Z}/p^m\mathbb{Z})[X]$, FOR GIVEN m.

2. (FINDING MAXIMAL ORDERS) LET $f \in \mathbb{Z}[X]$ MONIC WITH NON-ZERO DISCRIMINANT $\Delta(f)$ BE GIVEN. WRITE $\mathbb{Q}[\alpha]$ FOR THE $\mathbb{Q}$-ALGEBRA $\mathbb{Q}[X]/f\mathbb{Q}[X]$, WITH $\alpha = (X \bmod f)$. TO BE DETERMINED (A $\mathbb{Z}$-BASIS FOR) THE MAXIMAL ORDER A IN $\mathbb{Q}[\alpha]$, CONSISTING OF ALL $x \in \mathbb{Q}[\alpha]$ FOR WHICH $g(x) = 0$ FOR SOME MONIC $g \in \mathbb{Z}[X]$.

IF, IN PROBLEM 1, ONE HAS $\Delta(f) \not\equiv 0 \bmod p$, THEN FACTORING f IN $\mathbb{Z}_p[X]$ IS, BY HENSEL'S LEMMA, EQUIVALENT TO FACTORING $(f \bmod p)$ IN $(\mathbb{Z}/p\mathbb{Z})[X]$. SO PROBLEM 1 IS AT LEAST AS HARD AS FACTORING IN $(\mathbb{Z}/p\mathbb{Z})[X]$. FOR THE LATTER PROBLEM NO DETERMINISTIC POLYNOMIAL TIME ALGORITHM IS KNOWN. BUT THIS IS THE ONLY OBSTRUCTION AGAINST THE EXISTENCE OF A POLYNOMIAL TIME ALGORITHM FOR PROBLEM 1:

THEOREM 1. FACTORING IN $\mathbb{Z}_p[X]$ IS "DETERMINISTIC POLYNOMIAL TIME EQUIVALENT" TO FACTORING IN $(\mathbb{Z}/p\mathbb{Z})[X]$. (N.B.: m SHOULD BE ENCODED IN UNARY – THE OUTPUT HAS LENGTH AT LEAST m.)

CONSIDERING PROBLEM 2 FOR QUADRATIC f ONE FINDS THAT IT IS AT LEAST AS HARD AS FINDING LARGEST SQUARE DIVISORS OF INTEGERS. AGAIN, THIS IS THE ONLY OBSTRUCTION:

THEOREM 2. FINDING MAXIMAL ORDERS IS "DETERMINISTIC POLYNOMIAL TIME EQUIVALENT" TO FINDING LARGEST SQUARE DIVISORS OF INTEGERS.

THEOREM 2 FOLLOWS FROM WORK OF ZASSENHAUS. THEOREM 1 IS PROVED USING THE WELL KNOWN CONNECTION BETWEEN THE IRREDUCIBLE FACTORS OF f IN $\mathbb{Z}_p[X]$ AND THE PRIME POWER IDEAL FACTORS OF pA IN A.

TITLE: THE PRIMALITY TEST OF ADLEMAN AND HUANG

AUTHOR: H. W. LENSTRA, JR.

AFFILIATION: MATH
UNIV. OF CALIFORNIA
BERKELEY

IN THIS LECTURE THE BASIC INGREDIENTS ARE DISCUSSED THAT UNDERLIE THE PRIMALITY TEST OF ADLEMAN AND HUANG. THEY CLAIM THAT THEIR TEST RECOGNIZES PRIMES IN RANDOM POLYNOMIAL TIME.

THE TEST OF ADLEMAN AND HUANG IS OBTAINED BY REPLACING THE ELLIPTIC CURVES THAT APPEAR IN THE PRIMALITY TEST OF GOLDWASSER AND KILIAN BY ABELIAN VARIETIES OF DIMENSION 2. THESE ABELIAN VARIETIES ARE OBTAINED AS THE JACOBIANS OF HYPERELLIPTIC CURVES $y^2 = f(x)$, WHERE f HAS DEGREE 6.

THE ADVANTAGE OF THIS REPLACEMENT IS THAT THE RATHER STRONG UNPROVED RESULT THAT GOLDWASSER-KILIAN WOULD NEED (ON THE DISTRIBUTION OF PRIMES IN SHORT INTERVALS) IS REPLACED BY A WEAKER VERSION THAT HAS ACTUALLY BEEN PROVED (IWANIEC & JUTILA, 1979).

THE DISADVANTAGE OF THE REPLACEMENT IS THAT THE RECURSION GOES THE WRONG WAY; THE PRIMALITY PROOF FOR n IS REDUCED TO THE PRIMALITY PROOF OF A NUMBER n' THAT IS $\approx n^2$. WHAT HAS BEEN GAINED HOWEVER IS RANDOMNESS: n' IS MORE OR LESS RANDOM. AT DEPTH THREE IN THE RECURSION THE NUMBER $n''' \approx n^8$ TO BE PROVED PRIME IS <u>SO</u> RANDOM THAT IT IS REASONABLE TO EXPECT THAT n'''' CAN BE PROVED PRIME BY THE ORIGINAL GOLDWASSER-KILIAN TEST USING ELLIPTIC CURVES.

THE MOST DIFFICULT PART OF THE PROOF OF ADLEMAN AND HUANG IS TO SHOW THAT, IF A IS THE JACOBIAN OF A RANDOM HYPERELLIPTIC CURVE $y^2 = f(x)$, $\deg f = 6$, OVER $\mathbb{F}_p$, THEN $\# A(\mathbb{F}_p)$ IS, TO A CERTAIN EXTENT, UNIFORMLY DISTRIBUTED IN AN INTERVAL OF LENGTH $c \cdot p^{3/2}$ AROUND p^2. (THE ANALOGOUS STATEMENT FOR ELLIPTIC CURVES IS A STRAIGHTFORWARD CONSEQUENCE OF RESULTS OF DEURING (1942).)

TITLE: Algorithmic problems in geometry

AUTHOR: L. Lovász

AFFILIATION:

Geometry is perhaps the oldest branch of mathematics, and a great collection of beautiful result. However, if we are interested in the algorithmic aspects of the questions involved, then, in particular in higher dimensions, very little is known. These talks survey what is known and what is not known ~~the~~ about algorithmic aspects of two fundamental geometric structures, convex sets and lattices, and their inter-connections.

TITLE: *Homotopic River Routing*

AUTHOR: Kurt Mehlhorn

AFFILIATION: Saarbrücken

Abstract

Input: A set of non-intersecting curves in the Euclidian Plane

Output: A homotopic shift (the endpoints of the curves stay fixed and are considered as holes in the plane) of the curves such that any two curves have distance at least one.

We show that a simple flow condition is necessary and sufficient for the existance of a solution and give algorithms for testing the condition and constructing solutions.

TITLE: On Riemann's Zeta Function

AUTHOR: Andrew Odlyzko

AFFILIATION: AT+T Bell Laboratories
Murray Hill, NJ, USA

The complexity of computing the Riemann zeta function is of interest both because of the desire to verify the Riemann Hypothesis (RH) numerically for more zeros than have been done before as well as because ~~of~~ the ~~interest in the~~ ~~applicat~~ zeta function can be used ~~to~~ in efficient computation of some arithmetic functions. The best previously known algorithm for evaluating ~~the~~ $\zeta(\sigma+it)$ with σ bounded and t large to moderate accuracy ($\pm t^{-c}$ for some $c>0$, say) is based on the Riemann-Siegel formula and requires on the order of $t^{1/2}$ operations for each value that is computed. New algorithms, due to A. Schönhage and the speaker, enable one to compute any single value of $\zeta(\sigma+it)$ with σ fixed and $T \le t \le T+T^{1/2}$ to within $\pm t^{-c}$ in $T^{o(1)}$ operations on numbers of $O(\log T)$ bits, provided a precomputation involving ~~O(T)~~ $T^{1/2+o(1)}$ operations

TITLE:

AUTHOR:

AFFILIATION:

and $T^{1/2+o(1)}$ bits of storage is carried out beforehand. These algorithms lead to methods for numerically verifying the RH for the first n zeros in what is expected to be $n^{1+o(1)}$ operations (as opposed to about $n^{3/2}$ operations for the previous methods), as well as improved algorithms for the computation of various arithmetic functions such as $\pi(x)$. The new zeta function algorithms use the Fast Fourier Transform and a new method for the evaluation of certain rational functions. Various computations that have already been carried out or are planned will be described. Some of them have been used to test the plausibility of conjectures that go even beyond the RH and relate the distribution of spacings between consecutive zeros of the zeta function to that of energy levels in many-particle systems.

TITLE: *The Multiplicative Complexity of Pairs of Quadratic Boolean forms*

AUTHOR: Claus Peter Schnorr

AFFILIATION: Frankfurt

Abstract

For two quadratic boolean forms f_1, f_2 we characterize strict computational independence, in the sense that $L(f_1 \oplus f_2) = L(f_2)$, and weak computational independence, in the sense that $L(f_1, f_2) = L(f_1) + L(f_2)$ in terms of the dual domains of f_1, f_2. We give a polynomial time algorithm to compute $L(f_1, f_2)$ when the coefficients of f_1, f_2 are given.

(Joint work with R. Mirwald)

TITLE: GCD Computations

AUTHOR: Arnold Schönhage

AFFILIATION: Universität Tübingen

I/ As shown by the author in 1971, computing the gcd of N-bit integers is possible in time $O(N(\log N)^2 \log\log N)$, but there is the question for what size of N a corresponding algorithm really can beat order N^2 algorithms like "Lehmer's Method" with single precision precalculations (cf. Knuth, vol. 2). We report on a careful implementation of the asymptotically fast method (based on the notion of "controlled euclidean descent") which becomes actually faster for $N \geq 2400$, and which improves on the ordinary euclidean algorithm by a factor of about 10 in the range 40 000 – 100 000 for N. Operands of this size are, e.g., interesting with the application described in the next section.

II. The following probabilistic algorithm for the gcd D(x) of primitive integer polynomials A(x), B(x) of degree $\leq n$, with $|A|, |B| \leq 2^h$, is analyzed.

(0) Try (1) - (4) with t=h+1, 2h, 4h, 8h, ... until success.

(1) choose r at random, $0 \leq r < R = n(n+1)h$, set $\xi = 2^t + r$;

(2) compute $d(\xi) = \gcd(A(\xi), B(\xi))$;

(3) find $F_0 \in \mathbb{Z}[x]$ with coeff. $|f_j| < 2^{t-2}$ such that $F_0(\xi) = d(\xi)$, and set F(x) = primitive part of $F_0(x)$;

(4) if $F(x)|A(x)$ and $F(x)|B(x)$ then return $D(x) = F(x)$.

Termination is guaranteed by the worst case bound in

$\exists\, U(x), V(x) \in \mathbb{Z}[x] : U(x)A(x) + V(x)B(x) = QD(x)$ with $1 \leq Q < 2^{2nh}$,

which implies $d(\xi) = q(\xi)D(\xi)$ with $q(\xi)|Q$. The algorithm will succed in (3) and (4) iff $q(\xi) \cdot |D|_\infty < 2^{t-2}$, thus $q(\xi)$ should be small.

Prop: The arithmetic mean g of $\log q(\xi)$ over any sequence of $n(n+1)h$ consecutive integers is bounded by $g \leq n \log(nh) \cdot (\ln h + O(1))$.

This implies that the expected running time ~~(as for pointer machines)~~ is bounded by $E(T) \leq O(nh \log(nh) + n^2 \cdot \log^2(nh) \log h) \cdot \log(nh) \cdot \log\log(nh)$.

TITLE: SUBdominant Eigenvalues of Random d-graphs

AUTHOR: Eli Shamir (joint work with Andrei Broder)

AFFILIATION: Inst. of Math., Hebrew University Jerusalem, ISRAEL

Let G be a random graph of $G_{n,p}$, The average degree is $d = np$, assumed to be $\geq \log n$

Consider the eigenvalues λ_i, $1 \leq i \leq n$ of [the adjacency matrix of] G. The largest one is about d. For all the others:

$$|\lambda_i| = O(\sqrt{d}) \quad \underline{\text{with probability}} \ 1 - o(1), \ n \to \infty.$$

The main result concerns spaces of random d-regular graphs (or multigraphs) when d is fixed (so very sparse graphs) The estimate we prove is

(*) $i \geq 2$ implies $|\lambda_i| \leq 3 d^{3/4}$ $\underline{\text{with prob.}}$ $1 - O(e^{-\sqrt{d}})$

The proof consists in estimating the expected value $E\lambda_i$ (over the whole space) and using a martingale inequality to get the variance - or the deviation

TITLE:

AUTHOR: SHAMIR

AFFILIATION:

probability. (The variance $\sigma^2 = O(d)$).

The result can be extended to spaces where not only λ_1 $(=d)$ but also further eigenvalues (say λ_2) are sharply determined. Then the estimate (*) holds for all the other eigenvalues (say $i \geq 3$). These extensions have important applications in the design and rigorous analysis of quadratic optimization algorithms – E.g. for finding the "bisection width" of graphs (a recent work of Ravi Boppana)

The original estimate (*) for λ_2 yield a quick randomized construction of efficient expanden graphs.

TITLE: Complexity of Bilinear Problems.

AUTHOR: V. Strassen,

AFFILIATION: Zürich

This is a survey on asymptotic bilinear complexity. Everything is based on the notion of degeneration of bilinear maps. Asymptotic order and the asymptotic spectrum are introduced and in some cases (e.g. for $\mathbb{C}[T]/(F)$) the spectrum is computed. A variety of connections between asymptotic spectra and the exponent of matrix multiplication is exhibited.

TITLE: Finding Disjoint Paths on Expanders Graphs

AUTHOR: Eli Upfal

AFFILIATION: IBM San Jose

Abstract

In a typical parallel or distributed computation model processors are connected by a sparse interconnection network. To establish open-line communication between pairs of processors that wish to communicate interactively, a set of disjoint paths has to be constructed on the network. Since communication needs vary in time, paths have to be dynamically constructed and destroyed.

We study the complexity of constructing disjoint paths between given pairs of vertices on expander interconnection graphs. These graphs have been shown before to possess desirable properties for other communication tasks.

We present a sufficient condition for the existence of $K \leq n^{\rho}$ edge-disjoint paths connecting any set of K pairs of vertices on an expander graph. We then show that the computational problem of constructing these paths lies in the classes Deterministic-$\mathcal{P}$ and Random-$\mathcal{NC}$.

Furthermore, we show that the set of paths can be constructed in probabilistic polylog time in the parallel-distributed model of computation, in which the n participating processors reside in the nodes of the communication graph and all communication is done through edges of the graph. Thus, the disjoint paths are constructed in the very computation model that uses them.

Finally, we show how to apply variants of our parallel algorithms to find sets of *vertex-disjoint* paths when certain conditions are satisfied.

§ Supported in part by a Weizmann fellowship and by contract ONR N00014-85-C-0731

TITLE: Introduction to elliptic curves

AUTHOR: Don Zagier

AFFILIATION: Max-Planck-Institut für Mathematik
Bonn, FRG

The lecture gave a brief survey of some of the main results and questions in the arithmetic theory of elliptic curves. The two main parts of the theory concern the situation when one works over $\mathbb{Q}$ (or a number field) and the theory over $\mathbb{Z}/p\mathbb{Z}$ (or finite fields). The recent applications to factorization, primality testing, etc., have involved the latter; the lecture concentrated on the former.

An <u>elliptic curve</u> E over a field K can be given by a <u>Weierstrass equation</u> $y^2 = x^3 + Ax + B$ with $A, B \in K$; one denotes by $E(K)$ the set of points $(x,y) \in K^2$ satisfying this equation (plus an extra point O, the "point at infinity"). For $K = \mathbb{Q}$, the determination of $E(K)$ is a question of Diophantine equations. The key fact is that $E(K)$ has a group structure ($P+Q+R = O$ iff P, Q, R are collinear points; O is the null element); this reflects a method of constructing new solutions from old due to Diophantus (AD 250 ± 100) and Fermat (~ 1640). Moreover, this group is finitely generated (Mordell, 1916), i.e. it has the structure $\mathbb{Z}^r \oplus F$ where $r \geq 0$ is an integer called the <u>rank</u> and F a finite group. It is not known whether r can be arbitrarily large; it can be at least 14 (Mestre). The group F can be one of 15 groups $\mathbb{Z}/n\mathbb{Z}$ $(n = 1, 2, \ldots, 10, 12)$ or $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $(n = 2, 4, 6, 8)$ (Mazur 1977). An intuitively appealing definition of r is: the number of solutions $(x,y) \in E(\mathbb{Q})$ where the numerator and denominator of x are $\leq T$ has the asymptotic behavior $\sim c(\log T)^{r/2}$ as $T \to \infty$ for some real $c > 0$. The smallest solutions can be very large compared to the input data. For instance, a classical problem is the problem of <u>congruent numbers</u> (Fibonacci, 1225): a number n is called "congruent" if there exist three rational squares in arithmetic progression with difference n

TITLE: Elliptic Curves

AUTHOR: Zagier

AFFILIATION: MPI, Bonn

(e.g. 5 is congruent because $6\frac{97}{144}$, $11\frac{97}{144}$, $16\frac{97}{144}$ are squares), or equivalently if n is the area of a right triangle with rational sides. Then e.g. $n=157$ is congruent, but the rational squares in the smallest solution have almost 100-digit numerators and denominators.

Large solutions like this can be found using Fermat's "method of descent". For an important class of curves there is a second method. The curve E is called <u>modular</u> if it can be parametrized by modular functions, i.e. there exist modular functions $\xi(\tau)$, $\eta(\tau)$ ($\tau \in \mathbb{C}$, $\mathrm{Im}(\tau)>0$; "modular" means invariant under $\tau \to \frac{a\tau+b}{c\tau+d}$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in an appropriate subgroup of finite index of $SL_2(\mathbb{Z})$) which satisfy $\eta(\tau)^2 = \xi(\tau)^3 + A\xi(\tau) + B$ identically. Then for τ satisfying a quadratic equation over $\mathbb{Q}$, the values $\xi(\tau), \eta(\tau)$ are algebraic numbers, and adding the point $(\xi(\tau), \eta(\tau))$ of E to its algebraic conjugates (using the group law on E) one gets a rational point $P_H \in E(\mathbb{Q})$, the <u>Heegner point</u>. The hard part is to show $P_H \neq 0$. A recent success of this method was the theorem (Saito, 1986) that $2p$ is a sum of two rational cubes if p is a prime $\equiv 2 \pmod 9$, e.g. $22 = \left(\frac{25469}{9954}\right)^3 + \left(\frac{17299}{9954}\right)^3$. The Taniyama-Weil conjecture says that <u>every</u> modular curve over $\mathbb{Q}$ is modular; it has just been shown (Ribet, following Frey and Serre) that this implies Fermat's last theorem.

If we reduce the equation $y^2 = x^3 + Ax + B$ modulo p, where p is a prime dividing neither the denominators of A, B nor the discriminant $4A^3 + 27B^2$, then we get an elliptic curve over $\mathbb{Z}/p\mathbb{Z}$. Such a curve has $p+1-a_p$ points over $\mathbb{Z}/p\mathbb{Z}$, where a_p is an integer satisfying $|a_p| < 2\sqrt{p}$ (this is the result used in all the factorization and primality testing algorithms). A key invariant of the elliptic curve is the <u>L-series</u> $L(s) = \prod_p \frac{1}{1 - \frac{a_p}{p^s} + \frac{p}{p^{2s}}}$. If E is modular, this L-series is a holomorphic function of s in the entire complex plane, so we can

TITLE: Elliptic Curves

AUTHOR: Zagier

AFFILIATION: MPI

speak of κ, the order of vanishing of $L(s)$ at $s=1$. The deepest conjecture in the theory is the <u>Birch–Swinnerton-Dyer conjecture</u>, which says that $\kappa = r$ (the rank); in particular, $E(\mathbb{Q})$ is infinite if and only if $L(1)$ vanishes (intuitively, iff the number of points (mod p) is on average a little larger than $p+1$). Some partial results are known, e.g. using Heegner points, Gross and I (1983) showed that $\kappa = 1 \Rightarrow r \geq 1$ if E is modular, i.e. if $L(1)=0$ and $L'(1) \neq 0$ then the Diophantine equation $y^2 = x^3 + Ax + B$ must have a solution. A consequence of the Birch–Swinnerton-Dyer conjecture is a

<u>Conjectural Solution to the Problem of Congruent Numbers:</u>

Let $n \geq 0$ be squarefree and define $N_\pm$ by

(n even) $\left.\begin{matrix} N_+ \\ N_- \end{matrix}\right\}$ = number of solutions of $n = a^2+b^2+c^2$ with $c = \begin{cases} 4 \times \text{even number} \\ 4 \times \text{odd number} \end{cases}$

(n odd) $\left.\begin{matrix} N_+ \\ N_- \end{matrix}\right\}$ = number of solutions of $n = a^2+b^2+c^2$ with $b+c = \begin{cases} 4 \times \text{even number} \\ 4 \times \text{odd number} \end{cases}$.

Then n is congruent $\Leftrightarrow$ $N_+ = N_-$.

The direction $\Rightarrow$ is a consequence of results of Coates–Wiles and Waldspurger (Tunnell); the other direction has been checked up to $n=2000$.

Technical Sessions

TITLE: Tight bounds for the complexity of deterministic and randomized comparison sorting algorithms.

AUTHOR: Noga Alon

AFFILIATION: Dep. of Mathematics, Tel Aviv University, Tel Aviv, Israel and Bell Communications Research, Morristown, NJ, 07960, U.S.A.

We describe some recent results about the complexity of randomized and deterministic comparison parallel sorting algorithms. We show that the best running time of any parallel randomized or deterministic comparison algorithm that sorts n elements with p processors is $\Theta(\log n / \log(p/n))$ for $p > 2n$ and is $\Theta(\log n/(p/n))$ for $p \leq 2n$.

We further prove that for every fixed $k \geq 2$, $\Omega(n^{1+1/k} (\log n)^{1/k})$ processors are necessary ($O(n^{1+1/k} (\log n)^2$ are known to be sufficient) in any deterministic comparison algorithm that sorts n elements in k rounds, whereas the best randomized algorithm for sorting n elements in k rounds requires $\Theta(n^{1+1/k})$ processors.

TITLE: New techniques in primality testing

AUTHOR: Wieb Bosma

AFFILIATION: Universiteit van Amsterdam

Two applications are given of complex multiplication on elliptic curves to the theory of primality testing.
In the first, one replaces the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ of classical tests by the group of points on an elliptic curve admitting complex multiplication by the ring of integers of an imaginary quadratic number field. Just as a sufficient factorization of $n-1$ leads to primality proofs for n in the classical case, here one uses the factorization of $\mu-1$ in the complex multiplication ring to show that $\mu\bar{\mu}$ is a rational prime.
Secondly, one can speed up Atkin's primality test using complex multiplication. Instead of computing (rational) integral multiples of points on the elliptic curves employed here, one may multiply by elements of the imaginary quadratic complex multiplication ring (which are roughly half as large) – at least if the class number of the ring is one. It seems that with the proper reformulations, this class number condition can be dropped.

TITLE: Minimum information proofs of knowledge

AUTHOR: Gilles BRASSARD, David CHAUM and Claude CRÉPEAU

AFFILIATION: C. W. I., Amsterdam.

Assume P ("the Prover") knows a piece of information. This could be for instance the proof of some theorem or the prime factorization of some large integer. Assume further that P's information is <u>verifiable</u> in the sense that there exists an efficient (perhaps probabilistic) procedure capable of certifying the validity of the information. In order to convince V ("the Verifier") of this fact, P could simply show him the information and let him run the certifying procedure. This would however result in V knowing the information as well, so that he could subsequently show it to someone else and even claim it to be his.

In this talk, we discuss <u>minimum information protocols</u>, which allow P to convince V beyond any reasonable doubt that she has information that would pass the certifying procedure, but in a way that tells him nothing more. The main result is the existence of one such efficient protocol for which we can prove:

- No matter what V does, regardless of his computing power or luck, he will not learn anything about P's secret information. This statement is true in the strongest possible sense: the entire discussion between P and V conveys absolutely no information (in Shannon's sense) on P's secret!

- Except with an exponentially small probability, P will fail if she tries to convince V that she has this verifiable information when in fact she has not <u>unless</u> she succeeds in computing a large discrete logarithm while the protocol is in progress.

We also have protocols based on the intractability assumptions of factoring and of graph isomorphism, but they give an exponentially small probability for V to figure out P's secret.

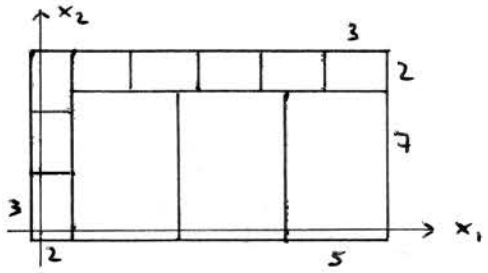
TITLE: The Complexity of Tiling Rectangles with Rectangles

AUTHOR: A. Clivio

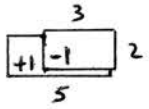
AFFILIATION: Mathematikdepartement, ETH Zürich, 8092 Zürich

<u>Definition.</u> Let $n \in \mathbb{N}^*$ $(:= \mathbb{N} \setminus \{0\})$;
$\mathbb{Z}[\underline{x}, \underline{x}^{-1}] := \mathbb{Z}[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$.
For $\underline{r} \in \mathbb{N}^{*n}$ (an "n-dimensional rectangle") we define the polynomial $f(\underline{r}) \in \mathbb{Z}[\underline{x}, \underline{x}^{-1}]$ by $f(\underline{r}) := \prod_{1 \le l \le n} \sum_{0 \le i \le r_l - 1} x_l^i$.
$g_1, \dots, g_k \in \mathbb{Z}[\underline{x}, \underline{x}^{-1}]$ is an integer tiling of $\underline{r}$ with $\underline{r}^{(1)}, \dots, \underline{r}^{(k)}$ if $\sum_{1 \le i \le k} g_i \cdot f(\underline{r}^{(i)}) = f(\underline{r})$; if all the coefficients of all the g_i's are 1, then the tiling is called a true tiling.

<u>Examples.</u> There is a true tiling of $(17,9)$ with $(2,3), (3,2), (5,7)$:
$(g_1 = 1 + x_2^3 + x_2^6,$
$g_2 = x_1^2 \cdot x_2^7 \cdot (1 + x_1^3 + x_1^6 + x_1^9 + x_1^{12}),$
$g_3 = x_1^2 \cdot (1 + x_1^5 + x_1^{10}).)$



There is an integer tiling of $(3,2)$ with $(2,2), (5,2)$:
$(g_1 = -x_1^2, \quad g_2 = 1.)$



The 1-dimensional true tilability problem, i.e.,

$$\bigcup_{0 \le k < \infty} \{ (r, r^{(1)}, \dots, r^{(k)}) \in \mathbb{N}^{*k+1} : \exists \text{ true tiling of } r \text{ with } r^{(1)}, \dots, r^{(k)} \},$$

is NP-complete; all the more, the n-dimensional true tilability problem is NP-hard (for every n).
On the other hand, for the n-dimensional integer tilability problem IT_n,

$$IT_n := \bigcup_{0 \le k < \infty} \{ (\underline{r}, \underline{r}^{(1)}, \dots, \underline{r}^{(k)}) \in \mathbb{N}^{*n \cdot (k+1)} : \exists \text{ integer tiling of } \underline{r} \text{ with } \underline{r}^{(1)}, \dots, \underline{r}^{(k)} \},$$

we have:

TITLE:

AUTHOR: A. Clivio

AFFILIATION:

<u>Theorem.</u> For every $n \in \mathbb{N}^*$: IT_n is in NP and in $coNP$.

<u>Remarks.</u> - The integers are given in binary notation.
- Of course, IT_1 is in P.

That IT_n belongs to $coNP$ follows from the

<u>Integer tilability criterion.</u> Let $n \in \mathbb{N}^*$, $\underline{r}, \underline{r}^{(1)}, \dots, \underline{r}^{(k)} \in \mathbb{N}^{*n}$.
There exists an integer tiling of $\underline{r}$ with $\underline{r}^{(1)}, \dots, \underline{r}^{(k)}$ iff
$\forall \pi : \{1, \dots, k\} \to \{1, \dots, n\}$ $\exists \ell$, $1 \le \ell \le n$, s.t.
$\gcd \{ r_\ell^{(i)} : \pi(i) = \ell \} \mid r_\ell$.
(F.W. Barnes, Algebraic Theory of Brick Packing II, Discrete Math. <u>42</u> (1982), Theorem 2.1.)

(Preprint available from the author.)

TITLE: Atkin's primality test

AUTHOR: Henri Cohen

AFFILIATION: University of Bordeaux I

The primality test of Goldwasser and Killian makes use of the following fundamental fact: if E is a random elliptic curve defined over $\mathbb{Z}/p\mathbb{Z}$ then its number of projective points $|E(\mathbb{Z}/p\mathbb{Z})|$ (which is between $p+1-2\sqrt{p}$ and $p+1+2\sqrt{p}$) has a reasonable chance of being of the form $2q$, where q is a pseudoprime to which the algorithm is applied recursively. The method is very important in theory, but is useless in practice as it is because it uses an algorithm of Schoof to compute $|E(\mathbb{Z}/p\mathbb{Z})|$ in $O(\log^8 p)$, and this is slow.

Atkin's idea is, instead of taking random elliptic curves, to take specific curves whose number of points modulo p is known a priori: the curves with complex multiplication.

A sketch of the algorithm is as follows: take the sequence of imaginary quadratic fields $K_1, K_2, \ldots$ ordered for instance by

TITLE: Atkin's primality test

AUTHOR: Henri Cohen

AFFILIATION: University of Bordeaux I

increasing class number. By computing a Jacobi symbol, test whether p (the number you are testing) splits in K_i. If yes, by Gaussian lattice reduction test whether p splits into principal ideals, say $p = \pi . \bar{\pi}$ (each time if the answer is no, take another field). Compute $p+1 \pm (\pi + \bar{\pi})$ and see if ~~they are~~ one of them is easy to factor and have a prime divisor $q > (p^{1/4}+1)^2$. If yes compute the j invariants of the elliptic curves with complex multiplication by K_i: to do this, compute numerically as a complex number with sufficiently high precision all the $h(K_i)$ conjugates of $j(O_{K_i})$, using well known power series expansions, and compute the symmetric functions modulo p. Theory tells you that the fact that $p = \pi\bar{\pi}$ implies that the polynomial that you obtain in this way splits completely into linear factors over $\mathbb{Z}/p\mathbb{Z}$. Using any Berlekamp type algorithm, compute any root j, and set $k = j/(j-1728)$ (a trivial modification is required if $j = 1728$ or 0 which can happen if $K_i = \mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}(\sqrt{-1})$)

TITLE: Atkin's primality test

AUTHOR: Henri Cohen

AFFILIATION: University of Bordeaux I

Then if c is any quadratic non residue mod p, one of the two curves

$$y^2 = x^3 + kx + k$$
$$y^2 = x^3 + kc^2x + kc^3$$

will have $p+1+(\pi+\bar{\pi})$ points mod p, and the other $p+1-(\pi+\bar{\pi})$. (Here again a modification is required for $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-1})$).

The rest of the algorithm is as in Goldwasser-Killian: you can very quickly find a point P on one of the curves and compute P^q and check whether this is O or not.

TITLE: Parallel Algorithms on Chordal Graphs

AUTHOR: Elias Dahlhaus / Marek Karpinski

AFFILIATION: Bonn

G is called <u>chordal</u> iff it contains no induced cycle > 3.

<u>Dirac</u>: G chordal iff any induced subgraph has a simplicial vertex x, (neighborhood of x forms a clique)

<u>Corollary</u>: Each chordal graph has at most as many (maximal) cliques as vertices.

<u>Results</u>: 1) The collection of all cliques can be computed in NC. [Naor, Naor, Schäffer] by Time, Processors $(O(\log^2 n), O(n^4))$.

2) For - free ~~graphs~~ chordal graphs the collection of its cliques can be computed in Time, Processors $(O(\log n), O(n^4))$.

G <u>strongly chordal</u>: $\Leftrightarrow$ its ~~edge~~ clique hypergraph is β-acyclic:

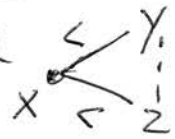
$\Leftrightarrow \nexists\ x_1 h_1 x_2 h_2 \ldots x_n h_n x_n, s, t,$
$x_i \in h_{i-1} \cap h_i$ and $x_i \notin h_k$, $k \neq i, i-1$

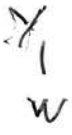
TITLE: chordal graphs (continuation)

AUTHOR: Dahlhaus

AFFILIATION:

<u>Farber</u>: G <u>strongly chordal</u>

$\Leftrightarrow$ $\exists$ order $<$, s.t. if  $\Rightarrow y - z$

and if $\Rightarrow$ 

Such an order is a <u>strongly perfect elimination ordering</u>

<u>Result</u>: Strongly perfect elimination orderings can be computed in NC

TITLE: Universal Hashing in VLSI

AUTHOR: Martin Fürer

AFFILIATION: Universität Zürich

A universal set of hashing functions is a collection $\{f_j : j \in J\}$ of functions $f_j : A \to B$ with the property

$$\forall x,y \quad x \neq y \Rightarrow \#\{j \in J : f_j(x) = f_j(y)\} \leq \frac{\#A}{\#B}.$$

For $F_2 = \mathbb{Z}/2\mathbb{Z}$ the linear functions $l : F_2^n \to F_2^{c \log n}$ form a very simple universal set of hashing functions. We use it to explore the difference between deterministic and Las Vegas VLSI computations.

Let a VLSI chip be divided by a short cut in two parts. Then the communication ~~across~~ the border is an essential issue for complexity. Consider the function f given by

$$f(x_1, \dots, x_n; y_1, \dots, y_n) = \begin{cases} 1 & \text{if } \exists j \; x_j = y_j \\ 0 & \text{otherwise} \end{cases}$$

with all $x_j \in \{0,1\}^n$ input on the left and all $y_j \in \{0,1\}^n$ input on the right side of the cut. Then by Mehlhorn and Schmidt [8] f cannot be computed deterministically before

TITLE: Universal Hashing in VLSI

AUTHOR: Martin Fürer

AFFILIATION: Universität Zürich

n^2 bits have crossed the border. On the other hand, if the computing agents on both sides can toss coins, an expected number of $O(n)$ bits is sufficient for every input with error probability 0. This bounds are optimal.

We define another function f_1 with the property that for every distribution of the input bits, much communication is necessary on the chip. Let $x_j = x_{j1}, \ldots, x_{jn}$ and $y_j = y_{j1}, \ldots, y_{jn}$.

$$f_1(x_1, \ldots, x_n, y_1, \ldots, y_n, s, l) = \begin{cases} 1 & \text{if } \exists j \; x_j = y_{j+l} \ldots, y_{j+l+s} \\ & \text{(with addition modulo } n) \\ 0 & \text{otherwise} \end{cases}$$

Let $N = \Theta(n^2)$ be the input length. Then every deterministic chip computing f_1 has the property $AT^2 = \Omega(N^2)$ (A = area, T = time), whereas a Las Vegas chip can solve this problem with $AT^2 = O(N \operatorname{poly}(\log N))$.

TITLE: Polynomial Decomposition Algorithms

AUTHOR: Susan Landau

AFFILIATION: Wesleyan University + Yale University

The question of when ~~[illegible]~~ can $f(x)$, a polynomial, be decomposed into $g(h(x))$, where degree $g(x)$, $h(x)$ ~~[illegible]~~ >1, is a fundamental one. In recent work, Barton and Zippel, and Alagar and Thanh gave (different) exponential algorithms. We give a polynomial time algorithm over any ring which contains an inverse of r, the degree of $g(x)$. We also give a new structure theorem which ~~gives~~ leads to an $n^{\log n}$ algorithm for irreducible polynomials over fields of char p, and a polynomial time algorithm for irreducible polynomials over finite fields.

This is joint work with Dexter Kozen.

We also report on some further developments by Joachim von zur Gathen and Matthew Dickerson.

TITLE: Optimal Algorithms for the Commutator of 2x2 - Matrices

AUTHOR: Roland Mirwald

AFFILIATION: Universität Frankfurt, Robert-Mayer-Str. 6-10
6000 Frankfurt, FRG

We consider the computational problem of computing the commutator $[A, B] := AB - BA$ of 2×2-matrices A and B over a field k with $\operatorname{char} k \neq 2$. It is known that this problem can be reduced to the case that we have matrices of trace 0, i.e. to the product in the Lie algebra $sl(2,k)$, and that the multiplicative complexity as well as the bilinear complexity (the rank) of this problem equals 5.

We investigate the set of optimal bilinear algorithms for $sl(2,k)$, the so-called algorithm variety of $sl(2,k)$. This is the set of all $(u_1, v_1, W_1, \dots, u_5, v_5, W_5)$ where $u_\varrho, v_\varrho \in sl(2,k)^*$, $W_\varrho \in sl(2,k)$ $(\varrho = 1, \dots, 5)$ s.t.

$$[A, B] = \sum_{\varrho=1}^{5} u_\varrho(A) v_\varrho(B) W_\varrho \quad \forall A, B \in sl(2,k).$$

The main result is that all these opt. bil. algorithms are equivalent in the following sense: A certain group of (linear) mappings - the extended isotropy group of $sl(2,k)$ - operates <u>transitivelly</u> on the algorithm variety of $sl(2,k)$.

This is analogous to the case of 2×2-matrix multiplication which has been treated by de Groote.

Reference: R. Mirwald: The Algorithmic Structure of $sl(2,k)$. Proc. AAECC-3, Springer Lect. Notes on Comp. Sc. No. ? (Ed.: Jacques Calmet).

TITLE: Probabilistic Communication

AUTHOR: Rüdiger Reischuk

AFFILIATION: Institut für Theoretische Informatik
Technische Hochschule Darmstadt

We consider the 2 processor communication model introduced by Yao. P_0 and P_1 cooperatively want to compute a function $f(X_0, X_1)$ where at the beginning X_i is only known to P_i. Different kinds of probabilistic protocols are defined characterized by the probability distribution (uniform - nonuniform), the amount of error and the number of communication rounds. The communication complexity of a function f is the number of bits exchanged by an optimal protocol for the worst input pair (x_0, x_1). Among others it is shown that for fixed error $\epsilon < \frac{1}{2}$ there can be an exponential difference between the probabilistic k and $(k-1)$ round communication complexity. On the other hand if ϵ may grow towards $1/2$ the complexity is almost identical for 1-round protocols and protocols with an arbitrary number of rounds.

Reference: B. Halstenberg, R. Reischuk, On Different Modes of Communication, TR 1987, TH Darmstadt

TITLE: A Deterministic Algorithm For Sparse Multivariate Polynomial Interpolation.

AUTHOR: Michael Ben-Or and Prasoon Tiwari

AFFILIATION: Jerusalem; IBM T.J. Watson Research Center Yorktown Heights, NY 10598

Consider a black box which contains a multivariate polynomial in n variables with at most k non-zero coefficients (in $\mathbb{C}$, for example). We are allowed to evaluate this polynomial at any point. We show that the polynomial can be completely determined by $2k$ evaluations, independent of its degree and n. The algorithm uses a BCH decoding technique, an a recent technique of Grigoriev and Karpinski.

TITLE: Separating Randomised Complexity Classes

AUTHOR: Rutger Verbeek

AFFILIATION: Univ. Bonn & Siemens AG

We discuss the fundamental question of separating bounded error probabilistic ("Monte Carlo") complexity classes. Since the "bounded error" property is a "semantic" one, there seems not to exist an enumerable subset of appropriately bounded machines forming some complexity class, as it is the case for deterministic, nondeterministic, and (unbounded error) probabilistic machines. Thus neither complete sets for classes like BPP (= Monte Carlo polynomial time) seem to exist nor standard diagonalization techniques can be applied. The only way of separating is by deterministic simulation and padding which works rather well for Monte Carlo space (via the squared space simulation of Borodin, Cook, and Pippenger we can prove e.g. Monte Carlo SPACE$(\log^p n) \subsetneq$ MC-SPACE$(\log^q n)$ iff $p<q$), but leaves almost exponential gaps in all other cases (i.e. MC-TIME, uniform MC circuit size, and uniform MC circuit depth). If we restrict ourself to "provable" Monte Carlo machines, for which the bounded error property is provable in some sound axiomatisable proof system (e.g. Peano Arithmetic), then the hierarchies become at least as dense as in the deterministic case; because we can use Monte Carlo constructible bounds, in some cases even denser. Such Monte Carlo (but not determ.) constructible bounds in fact exist (e.g. space bounds far below $\log\log n$). Another advantage of using provable classes is the existence of complete sets. E.g. the provable $\log^k n$-depth Monte Carlo circuit value problem is complete for provable RNC^k.

(Joint work with Marek Karpinski)

TITLE: Asymmetry and Efficient Randomized Computation

AUTHOR: Umesh Vazirani

AFFILIATION: U. C. Berkeley.

"Symmetric Breaking" is a basic function of randomization in computational tasks. This suggests a different notion of "pseudo-randomness" from polynomial time indistinguishability – namely, that a sequence is pseudo-random if it satisfies the symmetry breaking condition. Let p be a prime with 2 a primitive root mod p. Let $x, y \in GF(2)^p$. Then we conjecture that the sequence

$$x+y,\ x+\Pi(y),\ x+\Pi^2(y), \ldots, x+\Pi^k(y)$$

where Π denotes cyclic shift by one position, and $+$ denotes $GF(2)^p$ addition, is pseudo-random in the ~~sense~~ above sense.

The conjecture is based on the following theorem: the cyclic shifts of any ~~not~~ vector in $GF(2)^p$ distinct from 0^p & 1^p have $GF(2)$ rank at least

TITLE:

AUTHOR: U. Vazirani

AFFILIATION:

(2)

p-1; the invariant subspace consists of vectors of even parity. We use this property to prove the following result about extracting quasi-random sequences from two independent semi-random sources:

Let x and y be p-bits of output from two independent δ-semi-random sources. Let $b_i = x_i \circ \pi^i(y)$ where $\circ$ denotes GF(2) inner product. Then the sequence $b_0 b_1 \cdots b_{c(\delta)p}$ is quasi-random (i.e almost unbiased and independent bits). This improves upon the previous construction which extracted a single bit from $O(\lg n)$ source bits. Using fast fourier transform techniques, the new algorithm can be implemented in time $O(n \log\log n)$ to yield n quasi-random bits from $O(n)$ source bits.

TITLE: **Expected mistake bounds for on-line learning algorithms (extended abstract)**

AUTHOR: MANFRED WARMUTH

AFFILIATION: UNIVERSITY OF CALIFORNIA, SANTA CRUZ

Department of Computer and Information Sciences, University of California, Santa Cruz, California 95064.

Abstract. Valiant has introduced a model for learning concepts from random examples in which a concept class is polynomially learnable if there is a polynomial algorithm that creates a hypothesis that has small error with high probability. We consider a related on-line learning model in which the learning algorithm makes a prediction for each example before receiving its classification. Each such interaction is called a trial. If the prediction is incorrect, we say that the algorithm makes a mistake. We show that Valiant's model of polynomial learnability is equivalent to

a) requiring that there exists a polynomial on-line learning algorithm for which the probability of making a mistake at the i th trial has certain bounds or

b) requiring that there exists a polynomial on-line learning algorithm for which the expected total number of mistakes on a sequence of m trials has certain bounds.

We also introduce a model of space efficient learnability in which the space used by the learning algorithm must be polynomial in $log(m)$, where m is the number of trials. It is an open problem whether polynomial learnability implies space efficient polynomial learnability.

Joined work with David Haussler and Nick Littlestone

The authors gratefully acknowledge the support of ONR grant N00014-86-K-0454.

TITLE:

AUTHOR: AVI WIGDERSON

AFFILIATION:

In this talk I shall illustrate some of the techniques, ~~by showing three lower bounds~~ as well as the different nature of some members of the PRAM family by showing three lower bounds on computing Boolean functions by these models.

TITLE: LOWER BOUNDS ON PRAMs

AUTHOR: AVI WIGDERSON

AFFILIATION: HEBREW UNIVERSITY

The PRAM family of models has many member, that are usually distinguished by whether ~~they can~~ processors can simultaneously access a shared memory cell for a read or write operation. When write conflicts are allowed, different models handle them with different conflict resolution schemes.

Understanding the absolute and relative power of these models is essential for understanding in what way comunication limits parallel computation. In the last five years a variety of techniques for proving lower bounds on PRAMs were developed, that use adversary arguments, probabilistic methods, Ramsey theory, Kolmogorov complexity and more.