Lecture Notes in Computer Science 1046
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Advisory Board: W. Brauer D. Gries J. Stoer

Claude Puech Rüdiger Reischuk (Eds.)

# STACS 96

13th Annual Symposium
on Theoretical Aspects of Computer Science
Grenoble, France, February 22-24, 1996
Proceedings

Springer

Volume Editors

Claude Puech
iMAGIS-IMAG
BP 53, F-38041 Grenoble Cedex 09, France

Rüdiger Reischuk
Institut für Theoretische Informatik, Medizinische Universität zu Lübeck
Wallstr. 40, D-23560 Lübeck, Germany

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

**STACS <13, 1996, Grenoble>:**
Proceedings / STACS 96 / 13th Annual Symposium on Theoretical Aspects of Computer Science Grenoble, France, February 22 - 24, 1996. Claude Puech ; Rüdiger Reischuk (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1996
(Lecture notes in computer science ; Vol. 1046)

ISBN 3-540-60922-9
NE: Puech, Claude [Hrsg.]; GT

CR Subject Classification (1991): F, D.1, D.4, G.1-2, I.3.5, E.3

ISBN 3-540-60922-9 Springer-Verlag Berlin Heidelberg New York



Typesetting: Camera-ready by author
SPIN 10512627 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

# Foreword

The Symposium on Theoretical Aspects of Computer Science (STACS) is held annually, alternating between France and Germany. The STACS meeting is organized jointly by the Special Interest Group for Theoretical Computer Science of the Gesellschaft für Informatik (GI) in Germany and the Special Interest Group for Applied Mathematics of the Association Française des Sciences et Technologies de l'Information et des Systèmes (AFCET) in France.

STACS'96 is the thirteenth in this series, held in Grenoble, February 22-24, 1996. Previous STACS symposia were held in Paris (1984), Saarbrücken (1985), Orsay (1986), Passau (1987), Bordeaux (1988), Paderborn (1989), Rouen (1990), Hamburg (1991), Cachan (1992),Würzburg (1993), Caen (1994), München (1995).

For all of these symposia, the proceedings have been published in the Lecture Notes in Computer Science series of Springer-Verlag.

STACS has become one of the most important annual meetings in Europe for the theoretical computer science community. It covers a wide range of topics in the area of foundations of computer science. This year, 185 submissions with authors from more than 30 countries were received. A fair proportion of them came from non-European countries. Each submission was sent to three members of the program committee. In addition, each member of the program committee received the abstracts of all of the submitted papers. The program committee met for two days (October 27/28) in Paris and selected 54 out of the 185 submissions (29 %). Two submissions were then withdrawn by their authors, so the total numbers of submitted papers to be presented at the conference is 52. Because of the constraints imposed by the format of the conference, a number of good papers could not be accepted. The program committee was impressed by the high scientific quality of the submissions as well as the broad spectrum they covered within the area of theoretical computer science, including such topics as algorithms and data structures, automata and formal languages, computational complexity, computational geometry, cryptography, logic in computer science, semantics of programming languages, program specification, theory of parallel and distributed computation, parallel algorithms, theory of data bases, learning and verification.

The Program Committee consisted of L. Bougé (Lyon), V. Bruyère (Mons), H. Comon (Orsay), S. Fenner (Portland), A. Gibbons (Warwick), E. Grandjean (Caen), T. Hagerup (Saarbrücken), M. Krause (Dortmund),K.J. Lange (Tübingen), I. Litovky (Nice), C. Puech (Grenoble, co-chair), H. Reichel (Dresden), K. R. Reischuk (Lübeck, co-chair), P. Van Emde Boas (Amsterdam), S. Varrichio (L'Aquila). We wish to thank all the members of the program committee for their arduous work in evaluating the significance and scientific merits of the 185 submitted papers. Our gratitude extends to the numerous referees who assisted in this process.

We also thank the three invited speakers at this meeting, Gilles Brassard (Montréal), Joseph Sifakis (Grenoble), and Emo Welzl (Berlin) for accepting our invitation and sharing with us their insights on some new and very exciting developments in our area.

We thank the various sources who supported STACS'96, including CNRS, IMAG, INRIA, INPG, and UJF. A special tribute goes to AFCET and IMAG for their assistance in organizational matters related to this symposium.

Grenoble, January 1996

C. Puech

R. Reischuk

## List of Reviewers

Aiguier M.
Albers S.
Allender E.
Almeida J.
Alt H.
Amadio R.
Anantharaman S.
André C.
Anthony M.
Arnold A.
Audebaud P.
Brunie L.
Auletta V.
Auletta V.
Avenhaus J.
Azéma P.

Babai L.
Balcazar J.
Barth P.
Basin D.
Baude F.
Bauderon M.
Bäumker A.
Bean M.P.
Beaudouin-Lafon M.
Beauquier D.
Ben-David S.
Bernot G.
Berstel J.
Berthomé P.
Berthomieu B.
Bertot Y.
Bertram-Kretzberg C.
Bidoit M.
Blanchard F.
Bochert B.
Bodlaender H.
Bogdan M.
Boissonnat J.-M.
Bollig B.
Bond J.
Bonizzoni P.
Boudol G.
Boyd D.
Brandstädt A.
Breveglieri L.
Brüning H.K.
Buhrman H.
Buntrock G.

Cachera D.
Capelle C.
Carlet C.
Carton O.
Casas R.
Cechin A.
Chaudhuri S.
Choffrut C.
Clementi A.
Codenotti B.
Colson L.
Cosnard M.
Couveignes J.M.
Creignou N.
Crescenzi P.
Creutzburg R.
Crochemore M.
Culik II K.
Czumaj A.

Damm C.
Dauchet M.
De Santis A.
de Luca A.
de Rougemont M.
Delmas O.
Delorme M.
Deransart P.
Devilliers O.
Devolder J.
di Gesu V.
Diekert V.
Dietzfelbinger M.
Diks K.
Dittrich W.
Dubois C.
Dubois O.
Dulucq S.
Dunne P.
Duprat J.
Durand B.

Enjalbert P.
Eppstein D.
Esparza J.

Fages F.
Farinas L.
Fernandez M.
Fernandez-Baca D.
Fernau H.
Ferrand G.
Fischer P.
Flajolet P.
Flammini M.
Fleischer R.
Fraigniaud P.
Franchi-Zannettacci
Frederickson G.
Frougny C.

Gaujal B.
Gengler M.
Gergov J.
Gimenez E.
Goeppert J.
Goubault J.
Gräf A.
Green F.
Grigorieff S.
Grumbach S.
Guessarian I.

Habib M.
Hains G.
Hamann J.-C.
Hastad J.
Heckmann R.
Heise A.
Hertrampf U.
Holzer M.
Homeister T.
Homer S.
Hromkovic J.
Hromkovic J.
Hudelmaier J.
Hühne M.

Iliopoulos C.
Intrigila B.
Italiano G.

Jakoby A.
Janssens D.
Jouvelot P.

Kannan S.
Karpinski M.
Kenyon C.
Kesner D.

Kiehn A.
Kindler E.
Klasner N.
Klauck H.
Klein R.
Koiran P.
Kunde M.
Kutylowski M.
Kutylowski M.

Labahn R.
Lakhnech Y.
Lambert J.L.
Laroussinie F.
Latteux M.
Lauer H.
Lautemann C.
Le Gall P.
Lefmann H.
Lingas A.
Liskiewicz M.
Loescher
Loi M.
Lucks S.
Lutz J.
Lynch C.

Mader A.
Maffioli F.
Marion, J.-Y.
Martin B.
Martin E.
Mayordomo E.
Mayr E.
Mayr E.
Mazoyer J.
Meyer auf der Heide F.
Michaux C.
Michel P.
Mignosi F.
Mignot J.C.
Mignotte A.
Miguet S.
Möhring R.
Morvan M.
Mosses P. D.
Mundhenk M.

Muscholl A.
Muthukrishnan S.
Mutzel P.

Nanni U.
Nguyen-Huy X.
Niebert P.
Niedermeier R.
Niwinski D.

Panconesi A.
Paterson M.
Paulin C.
Pelligrini M.
Perennes S.
Perrin D.
Persiano G.
Persiano P.
Petit A.
Petrucci L.
Peyrat C.
Pietracaprina A.
Piston D.
Plaice J.
Pocchiola M.
Pointcheval D.
Pruim R.
Pucci G.

Radzik T.
Raman R.
Raman R.
Rauzy A.
Reinhardt K.
Restivo A.
Revol N.
Robson J.M.
Rossmanith P.
Rozoy B.

Santha M.
Sassone V.
Sauerhoff M.
Scheideler C.
Schill A.
Schindelhauer C.
Schirra S.

Schlick C.
Schmeck H.
Schnitger G.
Schnoebelen Ph.
Schoeling U.
Schöning U.
Seese D.
Sibeyn J.F.
Sieling D.
Simon H.U.
Simon I.
Smid M.
Sopena E.
Stephan F.
Stern J.
Strauss M.
Stren J.
Strong R.
Syska M.

Thiel C.
Thiemann P.
Thomas W.
Toran J.
Träff J.
Trevisan L.

Uhrig C.

Vallée B.
Vaudenay S.
Vauzeilles J.
Verbeek R.
Verchinine K.
Viennot L.

Waack S.
Wagner K.
Wagner K.
Wanka R.
Wegener I.
Wegner R.
Weis S.
Welzl E.
Wiehagen R.

Yvinec M.

Zhao Y.

# Table of Contents


## Invited Lecture

*New Trends in Quantum Computing*
G. Brassard (Univ. Montréal, CDN) 3

## Complexity Theory I

*Compressibility and Resource Bounded Measure*
H. Buhrman (CWI, NL), L. Longpré (Univ. Texas at El Paso, USA) 13

*On the Complexity of Random Strings*
M. Kummer (Univ. Karlsruhe, D) 25

## Automata Theory I

*Remarks on Generalized Post Correspondence Problem*
T. Harju, J. Karhumäki (Univ. Turku, SF), D. Krob (Univ. Paris VII, F) 39

*Cyclic Languages and Strongly Cyclic Languages*
M.-P. Béal (Univ. Denis Diderot, F), O. Carton (Univ. Marne-la-Vallée, F), C. Reutenauer (Univ. Québec à Montréal, CDN) 49

## Complexity Theory II

*Resource-Bounded Balanced Genericity, Stochasticity and Weak Randomness*
K. Ambos-Spies (Univ. Heidelberg, D), E. Mayordomo (Univ. Zaragoza, E), Y. Wang, X. Zheng (Univ. Heidelberg, D) 63

*The Complexity of Generating and Checking Proofs of Membership*
H. Buhrman (CWI, NL), T. Thierauf (Univ. Ulm, D) 75

*Observations on Measures and Lowness for $\Delta^p_2$*
J.H. Lutz (Iowa State Univ., USA) 87

*Solvable Black-Box Group Problems Are Low for PP*
V. Arvind, N.V. Vinodchandran (Inst. of Mathematical Sciences, IND) 99

## Automata Theory II

*Languages Recognized by Finite Aperiodic Groupoids*
M. Beaudry (Univ. Sherbrooke, CDN) 113

*Star-Height of an IN-Rational Series*
F. Bassino (Univ. Marne-la-Vallée, F) 125

*An Aperiodic Set of Wang Cubes*
K. Culik II (Univ. South Carolina, USA), J. Kari (Iterated Systems Inc., USA) 137

*Lyndon Factorization of Infinite Words*
G. Melançon (Univ. Bordeaux I, F) 147

## Parallel Algorithms

*Embedding Graphs with Bounded Treewidth into Optimal Hypercubes*
V. Heun, E.W. Mayr (Techn. Univ. München, D) 157

*Parallel Comparability Graph Recognition and Modular Decomposition*
M. Morvan, L. Viennot (Univ. Paris VII, F) 169

*Fault-Tolerant Shared Memory Simulations*
P. Berenbrink, F. Meyer auf der Heide, V. Stemann (Univ. Paderborn, D) 181

*On Word-Level Parallelism in Fault-Tolerant Computing*
P. Indyk (Stanford Univ., USA) 193

## Learning

*Learning with Confidence*
J. Barzdins, R. Freivalds (Univ. Latvia, LV),
C.H. Smith (Univ. Maryland, USA) 207

*Extracting Best Consensus Motifs from Positive and Negative Examples*
E. Tateishi, O. Maruyama, S. Miyano (Kyushu Univ. J) 219

*PAC Learning with Simple Examples*
F. Denis, C. D'Halluin, R. Gilleron (Univ. Lille I, F) 231

*General Inductive Inference Types Based on Linearly-Ordered Sets*
A. Ambainis, R. Freivalds (Univ. Latvia, LV),
C.H. Smith (Univ. Maryland, USA) 243

## Parallel and Distributed Systems I

*On the Power of Non-observable Actions in Timed Automata*
B. Bérard (ENS de Cachan, F), P. Gastin (Univ. Paris VII, F),
A. Petit (ENS de Cachan, F) 257

*Trace Rewriting: Computing Normal Forms in Time $O(n \log n)$*
M. Bertol, V. Diekert (Univ. Stuttgart, D) 269

*A Decision Procedure for Well-Formed Linear Quantum Cellular Automata*
C. Dürr, H. Lé Thanh, M. Santha (Univ. Paris-Sud, F) 281

## Complexity Theory III

*On the Complexity of Worst Case and Expected Time in a Circuit*
A. Jacoby, C. Schindelhauer (Univ. Lübeck, D) 295

*On the Existence of Hard Sparse Sets under Weak Reductions*
J.-Y. Cai (State Univ. New York at Buffalo, USA),
A.V. Naik (Univ. Chicago, USA),
D. Sivakumar (State Univ. New York at Buffalo, USA) 307

*Optimal Bounds on the Approximation of Boolean Functions with Consequences on the Concept of Hardness*
A.E. Andreev (Univ. Moscow, RU),
A.E.F. Clementi, J.D.P. Rolim (Univ. Geneva, CH) 319

*Fine Separation of Average Time Complexity Classes*
J.-Y. Cai, A.L. Selman (Univ. New York at Buffalo, USA) 331

## Invited Lecture

*Compositional Specification of Timed Systems*
J. Sifakis, S. Yovine 347

## Cryptography

*Optimal Tree-Based One-time Digital Signature Schemes*
D. Bleichenbacher, U.M. Maurer (ETH Zürich, CH) 363

*The Action of a Few Random Permutations on r-Tuples and an Application to Cryptography*
J. Friedman (Univ. British Columbia, CDN), A. Joux (CELAR, F), Y. Roichman (Massachussetts Inst. of Tech., USA), J. Stern (Ecole Normale Supérieure Paris, F), J.-P. Tillich (Univ. Caen, F) 375

*A Unified and Generalized Treatment of Authetication Theory*
U.M. Maurer (ETH Zürich, CH) 387

## Logic and Data Base Theory

*Monadic Second Order Logic on Tree-Like Structures*
I. Walukiewicz (Univ. Aarhus, DK) 401

*On Bijections vs. Unary Functions*
T. Schwentick (Univ. Mainz, D) 415

*The 3 Frenchmen Method Proves Undecidability of the Uniform Boundedness for Single Recursive Rule Ternary DATALOG Programs*
J. Marcinkowski (Univ. Wroclaw, PL) 427

## Algorithms I

*A Combinatorial Design Approach to MAXCUT*
T. Hofmeister, H. Lefmann (Univ. Dortmund, D) 441

*Characterizing the Complexity of Subgraph Isomorphism for Graphs of Bounded Path-Width*
A. Gupta (Simon Fraser Univ., CDN), N. Nishimura (Univ. Waterloo, CDN) 453

*A Charecterization of the Quadrilateral Meshes of a Surface which Admit a Compatible Hexahedral Mesh of Enclosed Volume*
S.A. Mitchell (Sandia National Laboratories, USA) 465

## Semantics and Program Verification

*On the Expressivity of the Modal Mu-Calculus*
J.C. Bradfield (Univ. Edinburgh, UK) 479

*Read-once Projections and Formal Circuit Verification with Binary Decision Diagrams*
B. Bollig, I. Wegener (Univ. Dortmund, D) 491

*"Optimal" Collecting Semantics for Analysis in a Hierarchy of Logic Program Semantics*
R. Giacobazzi (Univ. Pisa, I) 503

## Parallel and Distributed Systems II

*Flip-Flop Nets*
V. Schmitt (IRISA, F) 517

*Lower Bounds for Compact Routing*
E. Kranakis, D. Krizanc (Carleton Univ., CDN) 529

## Automata Theory III

*On the Successor Function in Non-classical Numeration Systems*
C. Frougny (Univ. Paris VIII, F) 543

*Minimal Forbidden Words and Symbolic Dynamics*
M.-P. Béal (Univ. Denis Diderot, F),
F. Mignosi, A. Restivo (Univ. Palermo, I) 555

## Algorithms II

*Universal Hashing and k-wise Independent Random Variables via Integer Arithmetic without Primes*
M. Dietzfelbinger (Univ. Dortmund, D) 569

*Ranking and Unranking Trees Using Regular Reductions*
P. Kelsen (Max-Planck Inst. für Informatik, Saarbrücken, D) 581

*On Competitive On-Line Paging with Lookahead*
D. Breslauer (Univ. Aarhus, DK) 593

*Hypothesis Testing in Perfect Phylogeny for a Bounded Number of Characters*
J. Lagergren (The Royal Inst. of Technology, Stockholm, S) 605

## Communication Complexity

*The "log Rank" Conjecture for Modular Communication Complexity*
C. Meinel (Univ. Trier, D), S. Waack (Georg-August Univ., Göttingen, D) 619

*Upper Bounds on Multiparty Communication Complexity of Shifts*
A. Ambainis (Univ. Latvia, LV) 631

*Some Bounds on Multiparty Communication Complexity of Pointer Jumping*
C. Damm, S. Jukna (Univ. Trier, D),
J. Sgall (Mathematical Inst., AV, Praha, CR) 643

*Optimal Schedules for d-D Grid Graphs with Communication Delays*
E. Bampis (Univ. Evry, F), C. Delorme (Univ. Paris-Sud, F),
J.-C. König (Univ. Evry, F) 655

## Invited Lecture

*Linear Programming - Randomization and Abstract Frameworks*
B. Gärtner, E. Welzl (Freie Univ. Berlin, D) 669

## Index of Authors

689