

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

Ugo Montanari José D.P. Rolim
Emo Welzl (Eds.)

Automata, Languages and Programming

27th International Colloquium, ICALP 2000
Geneva, Switzerland, July 9-15, 2000
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Ugo Montanari
University of Pisa, Department of Computer Sciences
Corso Italia, 40, 56125 Pisa, Italy
E-mail: ugo@di.unipi.it

José D.P. Rolim
University of Geneva, Center for Computer Sciences
24, Rue Général Dufour, 1211 Geneva 4, Switzerland
E-mail: Jose.Rolim@cui.unige.ch

Emo Welzl
ETH Zurich, Department of Computer Sciences
8092 Zurich, Switzerland
E-mail: emo@inf.ethz.ch

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Automata, languages and programming : 27th international colloquium ;
proceedings / ICALP 2000, Geneva, Switzerland, July 9 - 15, 2000. Ugo
Montanari . . . (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ;
Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2000
(Lecture notes in computer science ; Vol. 1853)
ISBN 3-540-67715-1

CR Subject Classification (1998): F, D, C.2-3, G.1-2

ISSN 0302-9743

ISBN 3-540-67715-1 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag is a company in the BertelsmannSpringer publishing group.
© Springer-Verlag Berlin Heidelberg 2000
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Steingraber Satztechnik GmbH, Heidelberg
Printed on acid-free paper SPIN: 10722141 06/3142 5 4 3 2 1 0

Preface

This volume contains the papers presented at the *27th International Colloquium on Automata, Languages and Programming (ICALP 2000)*, which took place at the University of Geneva, Switzerland, July 9–15, 2000.

The volume contains 69 contributed papers, selected by the two program committees from 196 extended abstracts submitted in response to the call for papers: 42 from 131 submissions for track A (Algorithms, Automata, Complexity, and Games) and 27 from 65 submissions for track B (Logic, Semantics, and Theory of Programming). Moreover, the volume includes abstracts of a plenary lecture by Richard Karp and of invited lectures by Samson Abramsky, Andrei Broder, Gregor Engels, Oded Goldreich, Roberto Gorrieri, Johan Håstad, Zohar Manna, and Kurt Mehlhorn.

The program committees decided to split the EATCS best paper awards among the following three contributions: *Deterministic algorithms for k -SAT based on covering codes and local search*, by Evgeny Dantsin, Andreas Goerdt, Edward A. Hirsch, and Uwe Schöning, *Reasoning about idealized Algol using regular languages*, by Dan R. Ghica and Guy McCusker, and *An optimal minimum spanning tree algorithm*, by Seth Pettie and Vijaya Ramachandran.

The best student paper award for track A was given to *Clique is hard to approximate within $n^{1-o(1)}$* , by Lars Engebretsen and Jonas Holmerin, and for track B to *On deciding if deterministic Rabin language is in Büchi class*, by Tomasz Fryderyk Urbanski.

We thank all of the authors who submitted papers, our invited speakers, the external referees we consulted, and the members of the program committees, who were:

Track A

- Peter Bro Miltersen, U. Aarhus
- Harry Buhrman, CWI Amsterdam
- Martin Dietzfelbinger, TU Ilmenau
- Afonso Ferreira, Inria Sophia Ant.
- Marcos Kiwi, U. Chile
- Jens Lagergren, KTH Stockholm
- Gheorghe Paun, Romanian Acad.
- Günter Rote, FU Berlin
- Ronitt Rubinfeld, NECI
- Amin Shokrollahi, Bell Labs
- Luca Trevisan, Columbia U.
- Serge Vaudenay, EPF Lausanne
- Emo Welzl, *Chair*, ETH Zürich
- Uri Zwick, Tel Aviv U.

Track B

- Rajeev Alur, U. Pennsylvania
- Rance Cleaveland, Stony Brook
- Pierpaolo Degano, U. Pisa
- Jose Fiadeiro, U. Lisbon
- Andy Gordon, Microsoft Cambridge
- Orna Grumberg, Technion Haifa
- Claude Kirchner, INRIA Nancy
- Ugo Montanari, *Chair*, U. Pisa
- Mogens Nielsen, U. Aarhus
- Catuscia Palamidessi, Penn. State
- Joachim Parrow, KTH Stockholm
- Edmund Robinson, QMW London
- Jan Rutten, CWI Amsterdam
- Jan Vitek, U. Geneva
- Martin Wirsing, LMU Munich
- Pierre Wolper, U. Liege

We gratefully acknowledge support from the Swiss National Science Foundation, from the computer science department of the University of Geneva, from the European agency INTAS, and from the EATCS. Finally, we would like to thank the local arrangement committee members – Olivier Powell, Frédéric Schütz, Danuta Sosnowska, and Thierry Zwissig – and Germaine Gusthiot for the secretarial support.

July 2000

Emo Welzl, Track A Program Chair
Ugo Montanari, Track B Program Chair
José D. P. Rolim, General Chair

Referees

Slim Abdennadher
Farid Ablayev
Luca Aceto
Susanne Albers
Eric Allender
Noga Alon
Eitan Altman
Rajeev Alur
Christoph Ambühl
Andris Ambainis
Artur Andrzejak
Farhad Arbab
Stefan Arnborg
Alfons Avermiddig
Yossi Azar
Evripidis Bampis
Nuno Barreiro
Lali Barriere
David Mix Barrington
Klaus Georg Barthelmann
Olivier Baudron
Martin Beaudry
Bruno Beauquier
Marco Bellia
Michael Bender
Nick Benton
Veronique Benzaken
Daniel Bleichenbacher
Peter van Emde Boas
Alexander Bockmayr
Chiara Bodei
Hans Bodlaender
Maria Bonet
Marcello Bonsangue
Michele Boreale
Vincent Bouchitté
Olivier Bournez
Peter Braß
Roberto Bruni
Peter Buergisser

Nadia Busi
Edson Caceres
Luis Caires
Sergio Campos
Giuseppe Castagna
Sébastien Choplin
Horatiu Cirstea
Rance Cleaveland
Andrea Clementi
Peter Clote
Philippe Codognet
Johanne Cohen
Jean-Sébastien Coron
Ricardo Corrêa
David Coudert
Ronald Cramer
Pierluigi Crescenzi
Felipe Cucker
Mads Dam
Ivan Damgaard
Olivier Danvy
Alain Darte
Nicola Rocco De
Pierpaolo Degano
Hartog Jerry Den
Theodosios Dimitrakos
Yevgeniy Dodis
Gilles Dowek
Frank Drewes
Jérôme Durand-Lose
Christoph Durr
Bruno Dutertre
Norbert Eisinger
Joost Engelfriet
Adam Eppendahl
Lea Epstein
Zoltan Esik
Javier Esparza
Kousha Etessami
Jean-Marc Fédou

VIII Referees

Uri Feige	Jaap-Henk Hoepman
Joan Feigenbaum	Frank Hoffmann
Sándor Fekete	Michael Hoffmann
Michael Fellows	Johan Holmerin
Stefan Felsner	Furio Honsell
Gianluigi Ferrari	Hendrik Jan Hoogeboom
Esteban Feuerstein	Jacob Howe
Jose Fiadeiro	Peter Hoyer
Lance Fortnow	Juraj Hromkovic
Cedric Fournet	Sebastian Hunt
Pierre Fraigniaud	Hans Huttel
Marcelo Frias	Johan Håstad
Roy Friedman	Sandy Irani
Bernd Gärtner	Lars Ivansson
Fabio Gadducci	Sanjay Jain
Anna Gal	Peter Jancar
Jérôme Galtier	David Janin
Juan Garay	Klaus Jansen
Max Garzon	Mark Jerrum
Bill Gasarch	Tania Jimenez
Cyril Gavoille	Öjvind Johansson
Rosario Gennaro	Bengt Jonsson
Giorgio Ghelli	Laurent Juban
Pablo Giambiagi	Gabriel Juhas
Leslie Goldberg	Sandrine Julia
Mikael Goldmann	Marcin Jurdzinski
Andy Gordon	Astrid Kaffanke
Roberto Gorrieri	Viggo Kann
Louis Granboulan	Juhani Karhumäki
Radu Grosu	Sagi Katz
Orna Grumberg	Sanjeev Khanna
Peter Grunwald	Joe Kilian
Sudipto Guha	Claude Kirchner
Venkatesan Guruswami	Alexander Knapp
Shai Halevi	Christian Knauer
Michael T. Hallett	Ulrich Kortenkamp
Mikael Hammar	Piotr Kosiuczenko
Therese Hardin	Jürgen Koslowski
Laura Heinrich-Litan	Ingolf Krüger
Matthew Hennessy	Klaus Kriegel
Jesper Gulmann Henriksen	Michael Krivelevich
Miki Hermann	Danny Krizanc
W. Hesselink	Hillel Kugler
Clemens Heuberger	Ravi Kumar

Gabriel Kuper
Orna Kupferman
Yassine Lakhnech
Francois Lamarche
Kim G. Larsen
Isabelle Guérin Lassous
Marina Lenisa
Stefano Leonardi
Francesca Levi
Paul Levy
Sebastien Limet
Huimin Lin
Luigi Liquori
Björn Lisper
Martin Loebel
Antonia Lopes
Jack Lutz
Andy Mück
Philip MacKenzie
Frederic Magniez
Pasquale Malacaria
Tal Malkin
Karina Marcus
Narciso Marti-Oliet
Bruno Martin
Simone Martini
GianCarlo Mauri
Elvira Mayordomo
Richard Mayr
Robert McNaughton
Klaus Meer
Lutz Meißner
Dieter van Melkebeek
Stephan Merz
Hermann Miki
Dale Miller
Joseph Mitchell
Michael Mitzenmacher
Faron Moller
Nicole Morawe
Matthew Morley
Till Mossakowski

Peter D. Mosses
Dalit Naor
Uwe Nestmann
Joachim Niehren
Mogens Nielsen
Flemming Nielson
Karl-Heinz Niggl
Isabel Nunes
Peter O'Hearn
Mitsu Ogiwara
Vadim Olshevsky
Luke Ong
Andre Osterloh
Rafi Ostrovsky
Catuscia Palamidessi
Daniel Panario
Joachim Parrow
Malacaria Pasquale
Christian Storm Pedersen
Dino Pedreschi
Samuele Pedroni
Andrezj Pelc
Paolo Penna
Stephane Perennes
Adriano Peron
Antoine Petit
Birgit Pfitzmann
Benny Pinkas
Andrew Pitts
Dennis Pixton
John Pliam
David Pointcheval
Katerina Pokozy
Carl Pomerance
Corrado Priami
Rosario Pugliese
Tal Rabin
Ivan Rapaport
Anna Redz
Oded Regev
Omer Reingold
Arend Rensink

Jürgen Richter-Gebert	Lothar Thiele
Søren Riis	Hayo Thielecke
Edmund Robinson	Thomas Thierauf
Mario Rodriguez-Artalejo	Wolfgang Thomas
Dana Ron	Mikkel Thorup
Roni Rosner	Simone Tini
Francesca Rossi	Jacobo Toran
Alex Russell	Leen Torenvliet
Jan Rutten	John Tromp
Alex Samorodnitsky	Daniele Turi
Tomas Sander	Christophe Tymen
Davide Sangiorgi	Staffan Ulfberg
Miklos Santha	Christian Urban
Vladimiro Sassone	Tomas Uribe
Uwe Schöning	Mark Van der Zwaag
Marcus Schaefer	Moshe Vardi
Berry Schoenmakers	Vasco Vasconcelos
K.U. Schulz	Santosh Vempala
Andreas Schulz	Betti Venneri
Philip Scott	Bjorn Victor
Francesca Scozzari	Paul Vitanyi
Sebastian Seiber	Jan Vitek
Maria Jose Serna	Uli Wagner
Peter Sewell	Michal Walicki
Detlev Sieling	John Watrous
Riccardo Silvestri	Ingo Wegener
Alex Simpson	Pascal Weil
Alistair Sinclair	Carola Wenk
Seppo Sippu	Benjamin Werner
D. Sivakumar	Susanne Wetzel
Carl Smith	Peter Widmayer
Warren Smith	Thomas Wilke
József Solymosi	Glynn Winskel
Dan Spielman	Martin Wirsing
Jiri Srba	Ronald de Wolf
Aravind Srinivasan	Pierre Wolper
Bernhard von Stengel	James Worrel
Bernd Sturmfels	Wang Yi
Harald Störrle	Mingsheng Ying
Madhu Sudan	Domenico Zambella
Amnon Ta-Shma	Francis Zane
Denis Therien	Leonid Zosin
P.S. Thiagarajan	

Table of Contents

Invited Talk:	1
Game Semantics: Achievements and Prospects <i>Samson Abramsky</i>	
Clique Is Hard to Approximate within $n^{1-o(1)}$	2
<i>Lars Engebretsen, Jonas Holmerin</i>	
Approximating the Independence Number and the Chromatic Number in Expected Polynomial Time	13
<i>Michael Krivelevich, Van H. Vu</i>	
Closed Types as a Simple Approach to Safe Imperative Multi-stage Programing	25
<i>Cristiano Calcagno, Eugenio Moggi, Walid Taha</i>	
A Statically Allocated Parallel Functional Language	37
<i>Alan Mycroft, Richard Sharp</i>	
An Optimal Minimum Spanning Tree Algorithm	49
<i>Seth Pettie, Vijaya Ramachandran</i>	
Improved Shortest Paths on the Word RAM	61
<i>Torben Hagerup</i>	
Improved Algorithms for Finding Level Ancestors in Dynamic Trees	73
<i>Stephen Alstrup, Jacob Holm</i>	
Lax Logical Relations	85
<i>Gordon Plotkin, John Power, Donald Sannella, Robert Tennent</i>	
Reasoning about Idealized ALGOL Using Regular Languages	103
<i>Dan R. Ghica, Guy McCusker</i>	
The Measurement Process in Domain Theory	116
<i>Keye Martin</i>	
Invited Talk:	127
Graph Transformation as a Conceptual and Formal Framework for System Modeling and Model Evolution <i>Gregor Engels, Reiko Heckel</i>	

Monotone Proofs of the Pigeon Hole Principle	151
<i>Albert Atserias, Nicola Galesi, Ricard Gavalda</i>	
Fully-Abstract Statecharts Semantics via Intuitionistic Kripke Models	163
<i>Gerald Lüttgen, Michael Mendler</i>	
Algebraic Models for Contextual Nets	175
<i>Roberto Bruni, Vladimiro Sassone</i>	
Asymptotically Optimal Bounds for OBDDs and the Solution of Some Basic OBDD Problems	187
<i>Beate Bollig, Ingo Wegener</i>	
Measures of Nondeterminism in Finite Automata	199
<i>Juraj Hromkovič, Juhani Karhumäki, Hartmut Klauck, Georg Schnitger, Sebastian Seibert</i>	
LTL Is Expressively Complete for Mazurkiewicz Traces	211
<i>Volker Diekert, Paul Gastin</i>	
An Automata-Theoretic Completeness Proof for Interval Temporal Logic .	223
<i>Ben C. Moszkowski</i>	
Invited Talk:	235
Which NP-Hard Optimization Problems Admit Non-trivial Efficient Approximation Algorithms?	
<i>Johan Håstad</i>	
Deterministic Algorithms for k -SAT Based on Covering Codes and Local Search	236
<i>Eugeny Dantsin, Andreas Goerdt, Edward A. Hirsch, Uwe Schöning</i>	
Closest Vectors, Successive Minima, and Dual HKZ-Bases of Lattices	248
<i>Johannes Blömer</i>	
Variable Independence, Quantifier Elimination, and Constraint Representations	260
<i>Leonid Libkin</i>	
Constraint Satisfaction Problems and Finite Algebras	272
<i>Andrei A. Bulatov, Andrei A. Krokhin, Peter Jeavons</i>	
An Optimal Online Algorithm for Bounded Space Variable-Sized Bin Packing	283
<i>Steven S. Seiden</i>	

Resource Augmentation for Online Bounded Space Bin Packing	296
<i>János Csirik, Gerhard J. Woeginger</i>	
Optimal Projective Algorithms for the List Update Problem.....	305
<i>Christoph Ambühl, Bernd Gärtner, Bernhard von Stengel</i>	
Efficient Verification Algorithms for One-Counter Processes.....	317
<i>Antonín Kučera</i>	
On the Complexity of Bisimulation Problems for Basic Parallel Processes .	329
<i>Richard Mayr</i>	
Decidable First-Order Transition Logics for PA-Processes.....	342
<i>Denis Lugiez, Philippe Schnoebelen</i>	
Invited Talk:.....	354
Non Interference for the Analysis of Cryptographic Protocols	
<i>Riccardo Focardi, Roberto Gorrieri, Fabio Martinelli</i>	
Average Bit-Complexity of Euclidean Algorithms.....	373
<i>Ali Akhavi, Brigitte Vallée</i>	
Planar Maps and Airy Phenomena	388
<i>Cyril Banderier, Philippe Flajolet, Gilles Schaeffer, Michèle Soria</i>	
Analysing Input/Output-Capabilities of Mobile Processes with a Generic Type System	403
<i>Barbara König</i>	
Information Flow vs. Resource Access in the Asynchronous Pi-Calculus...	415
<i>Matthew Hennessy, James Riely</i>	
Award Talk:.....	428
The Genomics Revolution and Its Challenges for Algorithmic Research	
<i>Richard M. Karp</i>	
Invited Talk:.....	429
Alternating the Temporal Picture for Safety	
<i>Zohar Manna and Henny B. Sipma</i>	
Necessary and Sufficient Assumptions for Non-interactive Zero-Knowledge Proofs of Knowledge for All NP Relations	451
<i>Alfredo De Santis, Giovanni Di Crescenzo, Giuseppe Persiano</i>	

Fast Verification of Any Remote Procedure Call: Short Witness-Indistinguishable One-Round Proofs for NP	463
<i>William Aiello, Sandeep Bhatt, Rafail Ostrovsky, S. Raj Rajagopalan</i>	
A New Unfolding Approach to LTL Model Checking	475
<i>Javier Esparza, Keijo Heljanko</i>	
Reasoning about Message Passing in Finite State Environments	487
<i>B. Meenakshi, R. Ramanujam</i>	
Extended Notions of Security for Multicast Public Key Cryptosystems....	499
<i>Olivier Baudron, David Pointcheval, Jacques Stern</i>	
One-Round Secure Computation and Secure Autonomous Mobile Agents .	512
<i>Christian Cachin, Jan Camenisch, Joe Kilian, Joy Müller</i>	
Round-Optimal and Abuse Free Optimistic Multi-party Contract Signing.	524
<i>Birgit Baum-Waidner, Michael Waidner</i>	
On the Centralizer of a Finite Set	536
<i>Juhani Karhumäki, Ion Petre</i>	
On the Power of Tree-Walking Automata	547
<i>Frank Neven, Thomas Schwentick</i>	
Determinization of Transducers over Infinite Words	561
<i>Marie-Pierre Béal, Olivier Carton</i>	
Invited Talk:	571
Constraint Programming and Graph Algorithms	
<i>Kurt Mehlhorn</i>	
Scalable Secure Storage when Half the System Is Faulty	576
<i>Noga Alon, Haim Kaplan, Michael Krivelevich, Dahlia Malkhi, Julien Stern</i>	
Generating Partial and Multiple Transversals of a Hypergraph	588
<i>Endre Boros, Vladimir Gurvich, Leonid Khachiyan, Kazuhisa Makino</i>	
Revisiting the Correspondence between Cut Elimination and Normalisation	600
<i>José Espírito Santo</i>	
Negation Elimination from Simple Equational Formulae	612
<i>Reinhard Pichler</i>	

Hardness of Set Cover with Intersection 1	624
<i>V.S. Anil Kumar, Sunil Arya, H. Ramesh</i>	
Strong Inapproximability of the Basic k -Spanner Problem	636
<i>Michael Elkin, David Peleg</i>	
Infinite Series-Parallel Posets: Logic and Languages.....	648
<i>Dietrich Kuske</i>	
On Deciding if Deterministic Rabin Language Is in Büchi Class.....	663
<i>Tomasz Fryderyk Urbański</i>	
On Message Sequence Graphs and Finitely Generated Regular MSC Languages.....	675
<i>Jesper G. Henriksen, Madhavan Mukund, K. Narayan Kumar, P.S. Thiagarajan</i>	
Invited Talk:.....	687
Pseudorandomness <i>Oded Goldreich</i>	
A Bound on the Capacity of Backoff and Acknowledgement-Based Protocols	705
<i>Leslie Ann Goldberg, Mark Jerrum, Sampath Kannan, Mike Paterson</i>	
Deterministic Radio Broadcasting	717
<i>Bogdan S. Chlebus, Leszek Gąsieniec, Anna Östlin, John Michael Robson</i>	
An ω -Complete Equational Specification of Interleaving	729
<i>W.J. Fokink, S.P. Luttik</i>	
A Complete Axiomatization for Observational Congruence of Prioritized Finite-State Behaviors.....	744
<i>Mario Bravetti, Roberto Gorrieri</i>	
Tight Size Bounds for Packet Headers in Narrow Meshes	756
<i>Micah Adler, Faith Fich, Leslie Ann Goldberg, Mike Paterson</i>	
Wavelength Assignment Problem on All-Optical Networks with k Fibres per Link	768
<i>Luciano Margara, Janos Simon</i>	
On the Logical Characterisation of Performability Properties	780
<i>Christel Baier, Boudewijn Haverkort, Holger Hermanns, Joost-Pieter Katoen</i>	

On the Representation of Timed Polyhedra.....	793
<i>Olivier Bournez, Oded Maler</i>	
Invited Talk:.....	808
Min-wise Independent Permutations: Theory and Practice	
<i>Andrei Z. Broder</i>	
Testing Acyclicity of Directed Graphs in Sublinear Time.....	809
<i>Michael A. Bender, Dana Ron</i>	
Computing the Girth of a Planar Graph.....	821
<i>Hristo N. Djidjev</i>	
Lower Bounds Are Not Easier over the Reals: Inside PH.....	832
<i>Hervé Fournier, Pascal Koiran</i>	
Unlearning Helps.....	844
<i>Ganesh Baliga, John Case, Wolfgang Merkle, Frank Stephan</i>	
Fast Approximation Schemes for Euclidean Multi-connectivity Problems..	856
<i>Artur Czumaj, Andrzej Lingas</i>	
Approximate TSP in Graphs with Forbidden Minors	869
<i>Michelangelo Grigni</i>	
Polynomial Time Approximation Schemes for General Multiprocessor Job Shop Scheduling	878
<i>Klaus Jansen, Lorant Porkolab</i>	
The Many Faces of a Translation.....	890
<i>Pierre McKenzie, Thomas Schwentick, Denis Thérien, Heribert Vollmer</i>	
Gales and the Constructive Dimension of Individual Sequences	902
<i>Jack H. Lutz</i>	
The Global Power of Additional Queries to p-Random Oracles.....	914
<i>Wolfgang Merkle</i>	
Homogenization and the Polynomial Calculus	926
<i>Josh Buresh-Oppenheim, Matt Clegg, Russell Impagliazzo, Toniann Pitassi</i>	
Author Index	939