

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

1380

Cláudio L. Lucchesi Arnaldo V. Moura (Eds.)

LATIN'98: Theoretical Informatics

Third Latin American Symposium
Campinas, Brazil, April 20-24, 1998
Proceedings



Springer

Series Editors

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

Volume Editors

Cláudio L. Lucchesi
Arnaldo V. Moura
University of Campinas, Institute of Computing
C.P. 6176, 13083-970 Campinas, SP, Brazil
E-mail: {lucchesi/arnaldo}@dcc.unicamp.br

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Theoretical informatics : proceedings / LATIN '98, Third Latin American Symposium, Campinas, Brazil, April 20 - 24, 1998.
Cláudio L. Lucchesi ; Arnaldo V. Moura (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1998
(Lecture notes in computer science ; Vol. 1380)
ISBN 3-540-64275-7

CR Subject Classification (1991): F1-3, E.3, G.1-2, I.1.1-2, I.3.5

ISSN 0302-9743

ISBN 3-540-64275-7 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 Berlin Heidelberg 1998
Printed in Germany

Typesetting: Camera-ready by author
SPIN 10631984 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

This volume is the proceedings of the International Conference LATIN'98, Latin American Theoretical INformatics, held in Campinas, Brazil, April 20–24, 1998.

This event is the third of a series started with LATIN'92, organized in São Paulo, Brazil, in April 1992, and continued with LATIN'95, organized in Valparaíso, Chile, in April 1995. The aim of the conference is to provide a high level forum for theoretical computer science research in Latin America, and to promote a strong and healthy interaction with the international scientific community.

The LATIN conferences focus on theory of computing, but in Latin America it is quite common to group under this umbrella fields which are sometimes classified otherwise, such as graph theory and combinatorics on words. After a lengthy and passionate discussion among the Program Committee members, papers on these subjects were considered. We hope that this policy will become a tradition in future editions of the conference. We received 53 submissions, from 104 authors in some 15 different countries. The 33 papers in this volume include 5 articles by invited speakers and 28 papers selected by the Program Committee based on some 160 reports filed by Committee members and other referees.

We would like to thank all individuals and organizations who cooperated with this event. In particular, the continued commitment of Springer-Verlag to publish the proceedings in its Lecture Notes in Computer Science series has strongly contributed to the success of this conference. We would also like to thank Imre Simon and Adriano Nagelschmidt Rodrigues who provided an intranet site for the Program Committee at the University of São Paulo, which proved to be essential for the multiple discussions among the PC members.

Undoubtedly LATIN is the main Latin American event in theoretical computer science. We feel confident that it is also gradually becoming a tradition in the computer science community.

April 1998

Cláudio L. Lucchesi
Program Chair

Arnaldo V. Moura
Program Vice-Chair

The Conference

Local Arrangements

The local arrangements for the conference were handled by the Institute of Computing of the University of Campinas (IC-UNICAMP), in Campinas, Brazil.

Organizing Committee

Ricardo de Oliveira Anido
Ariadne M. B. Rizzoni de Carvalho
Ricardo Dahab
Anamaria Gomide
Tomasz Kowaltowski

Cláudio L. Lucchesi (Chair)
Arnaldo V. Moura (Co-Chair)
Cândido F. Xavier de Mendonça Neto
Jorge Stolfi

Financial Support

FAPESP (State of São Paulo Research Funding Agency),
CNPq (Brazilian Council for Scientific and Technological Development),
CAPES Foundation (Brazilian Ministry of Education),
FAEP Foundation (University of Campinas), and
Institute of Computing (University of Campinas).

Cooperation

EATCS (European Association for Theoretical Computer Science),
SBC (Brazilian Computing Society),
SCCC (Chilean Computer Science Society),
SIGACT - ACM (Association for Computing Machinery),
SMCC (Mexican Computer Science Society), and
UMALCA (Mathematical Union of Latin America and Caribe).

Invited Speakers

Noga Alon (Tel Aviv Univ., Israel)
Richard Beigel (Lehigh Univ., USA)
Gilles Brassard (Univ. de Montréal, Canada)
Herbert Edelsbrunner (Univ. of Illinois, Urbana-Champaign, USA)
Juan A. Garay (IBM, Yorktown Heights, USA)

Program Committee

Ricardo Baeza-Yates (Univ. de Chile, Chile)
Valmir C. Barbosa (UFRJ, Brazil)
Richard Beigel (Lehigh Univ., USA)
Christian Choffrut (Univ. Paris VII, LITP, France)
Vašek Chvátal (Rutgers Univ., USA)
Volker Diekert (Univ. of Stuttgart, Germany)
Peter Eades (Univ. of Newcastle, Australia)
Herbert Edelsbrunner (Univ. of Illinois, Urbana-Champaign, USA)
Juan A. Garay (IBM, Yorktown Heights, USA)
Oscar Garrido (Univ. of Karlstad, Sweden)
Eric Goles (Univ. de Chile, Chile)
Jozef Gruska (Univ. of Brno, Czech Republik)
Katia Silva Guimarães (UFPE, Brazil)
Yoshiharu Kohayakawa (USP, Brazil)
Cláudio L. Lucchesi (UNICAMP, Brazil) (Chair)
Arnaldo V. Moura (UNICAMP, Brazil) (Co-Chair)
Gene Myers (Univ. of Arizona, USA)
Bruce Reed (CNRS, Paris VI, France)
Alexander Schrijver (CWI, Netherlands)
Peter Shor (ATT, USA)
Imre Simon (USP, Brazil)
János Simon (Univ. of Chicago, USA)
Jayme Luiz Szwarcfiter (UFRJ, Brazil)
Eli Upfal (Weizmann Inst., Israel and IBM, Almaden, USA)
Jorge Urrutia (Univ. of Ottawa, Canada)
Nivio Ziviani (UFMG, Brazil)

Referees

Amihood Amir
Sandra A. de Amo
David Applegate
Arnaldo de Albuquerque Araújo
Márcio Drummond Araújo
Amotz Bar-Noy
Saulo R. M. Barros
Mauro R. F. Benevides
Paulo Borba
Ljiljana Branković
Luboš Brim
Andrei Broder
Edson N. Cáceres
Rosa M. L. R. Carmo
Ivana Černá
Don Coppersmith
Ricardo Dahab
Javier Esparza
Antonio Elias Fabris
Martin Farach
Qin Wen Feng
Cristina Gomes Fernandes
Carlos E. Ferreira
Celina M. H. de Figueiredo
Luiz Henrique de Figueiredo
Marcelo Finger
Alan Frieze
Bill Gasarch
Leucio Guerra
Irene Guessarian
Edward Hermann Haesler
Matthias Jantzen
Esther Jennings
David Johnson
Ricardo Ueda Karpiscek
Alica Kelemenová

Sulamita Klein
Bernd Kreuter
Alain Lascoux
Pierre Lescanne
Stefan Lewandowski
Sérgio Lifschitz
Antonio Alfredo Loureiro
Nelson Maculan
Arnaldo Mandel
Célia Picinin de Mello
Lenka Motyčková
Edleno S. de Moura
Ian Munro
Anca Muscholl
Gonzalo Navarro
Valeria de Paiva
Tarcisio Pequeno
Roque Marinho Persiano
Holger Petersen
Rossella Petreschi
Yuval Rabani
Tal Rabin
Ed Reingold
Augusto Sampaio
João Carlos Setubal
Said Sidki
Flavio Soares Correa da Silva
Siang Wun Song
Dan Spielman
John Stembridge
Jean-Marc Steyaert
Jorge Stolfi
Routo Terada
Jacques Wainer
Yoshiko Wakabayashi
Jerzy Wojciechowski

Table of Contents

Algorithms, Complexity

| | |
|---------------------------------------------------------------------------------------------------------|----|
| Analysis of Rabin’s Polynomial Irreducibility Test | 1 |
| <i>Daniel Panario, Alfredo Viola</i> | |
| A Chip Search Problem on Binary Numbers | 11 |
| <i>Peter Damaschke</i> | |
| Uniform Service Systems with k Servers | 23 |
| <i>Esteban Feuerstein</i> | |
| Faster Non-linear Parametric Search with Applications to Optimization and Dynamic Geometry | 33 |
| <i>David Fernández-Baca</i> | |

Automata, Transition Systems, Combinatorics on Words

| | |
|-----------------------------------------------------------------------------|-----|
| Super-State Automata and Rational Trees | 42 |
| <i>Frédérique Bassino, Marie-Pierre Béal, Dominique Perrin</i> | |
| An Eilenberg Theorem for Words on Countable Ordinals | 53 |
| <i>Nicolas Bedon, Olivier Carton</i> | |
| Maximal Groups in Free Burnside Semigroups | 65 |
| <i>Alair Pereira do Lago</i> | |
| Positive Varieties and Infinite Words | 76 |
| <i>Jean-Éric Pin</i> | |
| Unfolding Parametric Automata | 88 |
| <i>Marcos Veloso Peixoto, Laurent Fribourg</i> | |
| Fundamental Structures in Well-Structured Infinite Transition Systems . . . | 102 |
| <i>Alain Finkel, Philippe Schnoebelen</i> | |

Computational Geometry, Graph Drawing

| | |
|----------------------------------------------------------------------------|-----|
| Shape Reconstruction with Delaunay Complex (Invited Paper) | 119 |
| <i>Herbert Edelsbrunner</i> | |
| Bases for Non-homogeneous Polynomial C_k Splines on the Sphere | 133 |
| <i>Anamaria Gomide, Jorge Stolfi</i> | |

The Splitting Number of the 4-Cube 141
*Luerbio Faria, Celina Miraglia Herrera de Figueiredo,
 Candido Ferreira Xavier de Mendonça Neto*

Short and Smooth Polygonal Paths..... 151
James Abello, Emden Gansner

Cryptography

Quantum Cryptanalysis of Hash and Claw-Free Functions (Invited Paper) . 163
Gilles Brassard, Peter Høyer, Alain Tapp

Batch Verification with Applications to Cryptography and Checking
 (Invited Paper) 170
Mihir Bellare, Juan A. Garay, Tal Rabin

Strength of Two Data Encryption Standard Implementations under
 Timing Attacks 192
Alejandro Hevia, Marcos Kiwi

Graph Theory, Algorithms on Graphs

Spectral Techniques in Graph Algorithms (Invited Paper)..... 206
Noga Alon

Colouring Graphs whose Chromatic Number Is Almost Their Maximum
 Degree..... 216
Michael Molloy, Bruce Reed

Circuit Covers in Series-Parallel Mixed Graphs 226
Orlando Lee, Yoshiko Wakabayashi

A Linear Time Algorithm to Recognize Clustered Planar Graphs and Its
 Parallelization 239
Elias Dahlhaus

A New Characterization for Parity Graphs and a Coloring Problem with
 Costs 249
Klaus Jansen

On the Clique Operator 261
Marisa Gutierrez, João Meidanis

Packet Routing

Dynamic Packet Routing on Arrays with Bounded Buffers 273
Andrei Z. Broder, Alan M. Frieze, Eli Upfal

On-Line Matching Routing on Trees 282
Alan Roberts, Antonios Symvonis

Parallel Algorithms

Analyzing Glauber Dynamics by Comparison of Markov Chains 292
Dana Randall, Prasad Tetali

The CREW PRAM Complexity of Modular Inversion 305
Joachim von zur Gathen, Igor Shparlinski

Communication-Efficient Parallel Multiway and Approximate Minimum
 Cut Computation 316
Friedhelm Meyer auf der Heide, Gabriel Terán Martínez

Pattern Matching, Browsing

The Geometry of Browsing (Invited Paper) 331
Richard Beigel, Egemen Tanin

Fast Two-Dimensional Approximate Pattern Matching 341
Ricardo Baeza-Yates, Gonzalo Navarro

Improved Approximate Pattern Matching on Hypertext 352
Gonzalo Navarro

Solving Equations in Strings: On Makanin's Algorithm 358
Claudio Gutiérrez

Spelling Approximate Repeated or Common Motifs Using a Suffix Tree . . . 374
Marie-France Sagot

Author Index 391