

Lecture Notes in Computer Science

2914

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer

Berlin

Heidelberg

New York

Hong Kong

London

Milan

Paris

Tokyo

Paritosh K. Pandya
Jaikumar Radhakrishnan (Eds.)

FST TCS 2003: Foundations of Software Technology and Theoretical Computer Science

23rd Conference
Mumbai, India, December 15-17, 2003
Proceedings



Springer

Series Editors

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

Volume Editors

Paritosh K. Pandya
Jaikumar Radhakrishnan
Tata Institute of Fundamental Research
School of Technology and Computer Science
Homi Bhabha Road, Mumbai 400005, India
E-mail: {pandya,jaikumar}@tifr.res.in

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

CR Subject Classification (1998): F.3, D.3, F.4, F.2, F.1, G.2

ISSN 0302-9743

ISBN 3-540-20680-9 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 part of Springer Science+Business Media

springeronline.com

© Springer-Verlag Berlin Heidelberg 2003
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 10973400 06/3142 5 4 3 2 1 0

Preface

Over the past two decades, the Foundations of Software Technology and Theoretical Computer Science (FSTTCS) conferences have been providing an annual forum in India for the presentation and publication of results in computer science from around the world. This volume contains the proceedings of the 23rd FSTTCS, organized under the aegis of the Indian Association for Research in Computing Science (IARCS).

FSTTCS 2003 attracted over 160 submissions from 29 countries. After obtaining 521 referee reports within a period of one month, the programme committee accepted 33 contributed papers, the maximum that could fit into a two-and-a-half-day programme. Unfortunately, many good papers had to be turned away. We thank all the authors for submitting their papers to FSTTCS 2003. We thank the reviewers for the tremendous support they provided to the conference through their informed and thorough reviews of the papers. We sincerely thank the members of the programme committee for lending their names to the conference and for meeting the challenge arising out of the increased number of submissions this year. We are especially grateful to Kamal Lodaya who came down to Mumbai to assist us during the PC meeting.

FSTTCS programmes have always featured highly eminent computer scientists as invited speakers. It is our great pleasure to thank the invited speakers of FSTTCS 2003, Randal Bryant, Moni Naor, Joseph Sifakis, Osamu Watanabe and Avi Wigderson, who graciously agreed to speak at the conference and contribute to this volume.

For several years now, topical workshops have been organized together with FSTTCS conferences. This year, the conference was preceded by a workshop on *Advances in Model Checking*, and was followed by a workshop on *Algorithms for Processing Massive Data Sets*. We thank the organizers and speakers for agreeing to come and share their expertise.

The PC meeting was held electronically using software originally developed by V. Vinay. We thank our colleagues at the Tata Institute of Fundamental Research who came forward to help us, in particular, Vishwas Patil, who got the software up and kept the system running. We thank the Department of Computer Science, IIT Bombay, for hosting the conference. We thank Springer-Verlag for agreeing to publish the proceedings of this conference, and its editorial team for helping us bring out this volume.

October 2003

Paritosh Pandya and
Jaikumar Radhakrishnan

Organization

The 23rd FSTTCS conference was organized by the Department of Computer Science and Engineering, Indian Institute of Technology, Bombay.

Programme Committee

R. Alur (University of Pennsylvania)	P.K. Pandya
V. Arvind (IMSc, Chennai)	(TIFR, Mumbai, Co-chair)
M. Charikar (Princeton University)	S. Prasad (IIT Delhi)
T. Dey (Ohio State University)	J. Radhakrishnan
J. Esparza (University of Stuttgart)	(TIFR, Mumbai, Co-chair)
S. Ghosh (TIFR, Mumbai)	S.K. Rajamani
M. Halldórsson (University of Iceland)	(Microsoft Research, Redmond)
H. Karloff (AT&T Labs, Research)	S. Sen (IIT Delhi)
K. Lodaya (IMSc, Chennai)	D. Sivakumar (IBM Almaden)
P.B. Miltersen (BRICS, Aarhus)	G. Sivakumar (IIT Bombay)
J. Mitchell (Stanford)	Th. Wilke (University of Kiel)
P. O'Hearn (Queen Mary, London)	U. Zwick (Tel Aviv University)

Organizing Committee

S. Chakraborty (CSE, IIT Bombay)	H.V. Sahasrabudhe
S. Chandran (CSE, IIT Bombay)	(KReSIT, IIT Bombay)
S. Patkar (Mathematics, IIT Bombay)	M. Sohoni (CSE, IIT Bombay, Chair)
A. Ranade (CSE, IIT Bombay)	S. Vishwanathan (CSE, IIT Bombay)

Referees

B. Adsul	E. Asarin	S. Biswas
P. Agarwal	Y. Azar	B. Blanchet
G. Agnarsson	M. Béal	A. Blum
M. Agrawal	R. Balasubramanian	D. Bošnački
R. Alexander	R. Banach	J. Borgström
E. Allender	M. Banerjee	V. Borkar
T. Amtoft	S. Banerjee	A. Bouajjani
V. Anantharam	Z. Bar-Yossef	G. Boudol
R. Anderson	J. Berdine	P. Bouyer
E. Arkin	M. Bern	M. Bozga
S. Arya	J.C. Birget	J. Bradfield

R. Bruni	C. Ghidini	J. Kari
C. Calcagno	J. Giesl	A. Karlin
G. Calinescu	R.J. van Glabbeek	D. Kaynar
A. Cau	G. Gopalakrishnan	A. Kesselman
S. Chaki	V. Goranko	R. Khandekar
S. Chakraborty	S. Graf	S. Khanna
T. Chan	J. Gramm	S. Khot
B. Chandra	D.P. Guelev	E. Kindler
M. Chang	H. Guo	T. Knapik
D. Charles	V. Guruswami	J. Koebler
C. Chekuri	H. Hüttel	B. Koenig
C. Choffrut	S. Haar	G. Kortsarz
A. Cimatti	N. Halbwachs	R. Kossak
A. Condon	B.V. Halldórsson	M. Koutny
B. Courcelle	S. Har-Peled	E. Koutsoupias
J. Couvreur	R. Hariharan	P. Kouznetsov
M. Datar	K. Heljanko	R. Krauthgamer
A.K. Datta	T. Herman	S.N. Krishna
A. Datta	P. Hines	M. Krivelevich
K. Deb	E.A. Hirsch	D. KroB
M. Dekhtyar	K. Honda	A. Kshemkalyani
G. Delzanno	P. Hoyer	A. Kucera
S. Demri	G. Huet	M. Kudlek
J. Desharnais	A. Hulgeri	R. Kuesters
B. Devereux	P. Indyk	W. Kuich
T. Dey	K. Iwama	K. Kumar
V. Diekert	S. Iyer	R. Kumar
H. Dierks	R. Jagadeesan	S. Kumar
A.A. Diwan	R. Jain	V. Kuncak
D. Dubhashi	S. Jain	O. Kupferman
K. Etessami	R. Janardan	P.P. Kurur
E. Even-Dar	D. Janin	D. Kuske
R. Fagerberg	T. Jayram	C. Löding
B. Farwer	R.M. Jensen	S. Lahiri
D. Feitelson	R. Jhala	M. Langberg
S. Fenner	R. Jothi	M. Laumanns
J. Flum	T. Junttila	V. Laviano
L. Fortnow	M. Jurdzinski	R. Leino
M. Fränzle	M. Kacprzak	H. Lin
G.S. Frandsen	B. Kalyanasundaram	Z. Liu
T. Fujito	S. Kamara ju	M. Lohrey
S. Funke	S. Kannan	S.V. Lokam
H. Gao	H. Kaplan	J. Longley
N. Garg	D. Kapur	G. Lowe
P. Gastin	J. Karhumaki	M. Müller-Olm

P. Madhusudan	J. Power	S. Sivasubramanian
M. Mahajan	S. Prasad	A. Stefanescu
S. Mahajan	R. Pucella	M. Steinby
R. Majumdar	X. Qiwen	M. Stoelinga
J.A. Makowsky	P. Quaglia	S.D. Stoller
S. Maneth	N. Raja	H. Straubing
D. Manjunath	S. Rajasekaran	O. Strichman
Y. Mansour	I.V. Ramakrishnan	C.R. Subramanian
J. Marion	K. Ramamritham	S. Sudarshan
U. Martin	R. Raman	S.P. Suresh
R. Mayr	V. Raman	H. Sverrisson
B. Meenakshi	R. Ramanujam	M. Turuani
S. Mehta	S. Ramesh	A. Ta-Shma
D. van Melkebeek	A. Ranade	K. Talwar
M. Mohri	R. Ravi	P. Tesson
F. Moller	J. Rehof	P.S. Thiagarajan
B. Moszkowski	J.D. Rogers	W. Thomas
M. Mukund	T. Roughgarden	A. Toley
M. Musuvathi	A. Russell	S. La Torre
K. Nakano	J. Rutten	R. Treffer
P. Narendran	A. Samorodnitsky	E. Tronci
A. Nayak	C. Sanchez	K. Varadarajan
Z.L. Nemeth	D. Sangiorgi	Moshe Y. Vardi
U. Nestmann	S. Sankaranarayanan	V.N. Variyam
R. De Nicola	H. Saran	M. Vaziri
M. Nielsen	S. Sarawagi	M. Veanes
S. Nishimura	M. Satpathy	M.N. Velez
G. Norman	A. Schaffer	R. Verma
L. O'Callaghan	C. Schindelhauer	B. Victor
H. Ohsaki	P. Schnoebelen	T. Vijayaraghavan
T. Ono	C. Schröter	S. Vishwanathan
M. Pagnucco	R. Schuler	D.P. Walker
S.P. Pal	T. Schwentick	I. Walukiewicz
R. Palmer	S. Schwoon	S. Weirich
R. Parikh	A. Sen	R. Wenger
A. Pavan	H. Shachnai	D.P. Williamson
W. Penczek	J. Shallit	L. Wischik
T. Perst	P. Shankar	R. de Wolf
H. Petersen	A. Shioura	P. Wolper
A. Petit	V. Shmatikov	M. Wooldridge
M. Pistore	W. Shukla	Y. Xie
N. Piterman	J.F. Sibeyn	C. Yap
W. Plandowski	A. Singh	B. Zhu
A. Pnueli	A. Sinha	W. Zielonka
S. Porschen	R. Siromoney	

Table of Contents

Contributed Papers

A Cryptographically Sound Security Proof of the Needham-Schroeder-Lowe Public-Key Protocol	1
<i>Michael Backes, Birgit Pfitzmann</i>	
Constructions of Sparse Asymmetric Connectors	13
<i>Andreas Baltz, Gerold Jäger, Anand Srivastav</i>	
A Separation Logic for Resource Distribution	23
<i>Nicolas Biri, Didier Galmiche</i>	
An Equational Theory for Transactions	38
<i>Andrew P. Black, Vincent Cremet, Rachid Guerraoui, Martin Odersky</i>	
Axioms for Regular Words	50
<i>Stephen L. Bloom, Zoltán Ésik</i>	
1-Bounded TWA Cannot Be Determinized	62
<i>Mikołaj Bojańczyk</i>	
Reachability Analysis of Process Rewrite Systems	74
<i>Ahmed Bouajjani, Tayssir Touili</i>	
Pushdown Games with Unboundedness and Regular Conditions	88
<i>Alexis-Julien Bouquet, Oliver Serre, Igor Walukiewicz</i>	
Real-Time Model-Checking: Parameters Everywhere	100
<i>Véronique Bruyère, Jean-François Raskin</i>	
The Caucal Hierarchy of Infinite Graphs in Terms of Logic and Higher-Order Pushdown Automata	112
<i>Arnaud Carayol, Stefan Wöhrle</i>	
Deciding the Security of Protocols with Diffie-Hellman Exponentiation and Products in Exponents	124
<i>Yannick Chevalier, Ralf Küsters, Michaël Rusinowitch, Mathieu Turuani</i>	
Subtyping Constraints in Quasi-lattices	136
<i>Emmanuel Coquery, François Fages</i>	

An Improved Approximation Scheme for Computing Arrow-Debreu Prices for the Linear Case	149
<i>Nikhil R. Devanur, Vijay V. Vazirani</i>	
Word Equations over Graph Products	156
<i>Volker Diekert, Markus Lohrey</i>	
Analysis and Experimental Evaluation of a Simple Algorithm for Collaborative Filtering in Planted Partition Models	168
<i>Devdatt Dubhashi, Luigi Laura, Alessandro Panconesi</i>	
Comparing Sequences with Segment Rearrangements	183
<i>Funda Ergun, S. Muthukrishnan, S. Cenk Sahinalp</i>	
On Logically Defined Recognizable Tree Languages	195
<i>Zoltán Ésik, Pascal Weil</i>	
Randomized Time-Space Tradeoffs for Directed Graph Connectivity	208
<i>Parikshit Gopalan, Richard J. Lipton, Aranyak Mehta</i>	
Distance-Preserving Approximations of Polygonal Paths	217
<i>Joachim Gudmundsson, Giri Narasimhan, Michiel Smid</i>	
Joint Separation of Geometric Clusters and the Extreme Irregularities of Regular Polyhedra	229
<i>Sumanta Guha</i>	
On the Covering Steiner Problem	244
<i>Anupam Gupta, Aravind Srinivasan</i>	
Minimality Results for the Spatial Logics	252
<i>D. Hirschkoff, É. Lozes, D. Sangiorgi</i>	
Algorithms for Non-uniform Size Data Placement on Parallel Disks	265
<i>Srinivas Kashyap, Samir Khuller</i>	
Efficient Algorithms for Abelian Group Isomorphism and Related Problems	277
<i>T. Kavitha</i>	
Quasi-polynomial Time Approximation Algorithm for Low-Degree Minimum-Cost Steiner Trees	289
<i>Jochen Könemann, R. Ravi</i>	
Model Checking and Satisfiability for Sabotage Modal Logic	302
<i>Christof Löding, Philipp Rohde</i>	
Merging and Sorting By Strip Moves	314
<i>Meena Mahajan, Raghavan Rama, Venkatesh Raman, S. Vijayakumar</i>	

The Macro Tree Transducer Hierarchy Collapses for Functions of Linear Size Increase	326
<i>Sebastian Maneth</i>	
Distributed Games	338
<i>Swarup Mohalik, Igor Walukiewicz</i>	
Maintenance of Multidimensional Histograms	352
<i>S. Muthukrishnan, Martin Strauss</i>	
Tagging Makes Secrecy Decidable with Unbounded Nonces as Well	363
<i>R. Ramanujam, S.P. Suresh</i>	
Quantum and Classical Complexity Classes: Separations, Collapses, and Closure Properties	375
<i>Holger Spakowski, Mayur Thakur, Rahul Tripathi</i>	
On the Greedy Superstring Conjecture.....	387
<i>Maik Weinard, Georg Schnitger</i>	
Invited Papers	
Reasoning about Infinite State Systems Using Boolean Methods	399
<i>Randal E. Bryant</i>	
Stringent Relativization.....	408
<i>Jin-Yi Cai, Osamu Watanabe</i>	
Component-Based Construction of Deadlock-Free Systems	420
<i>Gregor Gössler, Joseph Sifakis</i>	
Moderately Hard Functions: From Complexity to Spam Fighting	434
<i>Moni Naor</i>	
Zigzag Products, Expander Constructions, Connections, and Applications.....	443
<i>Avi Wigderson</i>	
Author Index	445