

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Jin-Yi Cai S. Barry Cooper
Hong Zhu (Eds.)

Theory and Applications of Models of Computation

4th International Conference, TAMC 2007
Shanghai, China, May 22-25, 2007
Proceedings

Volume Editors

Jin-Yi Cai

University of Wisconsin, Madison, Computer Sciences Department

1210 West Dayton Street, Madison, WI 53706, USA

E-mail: jyc@cs.wisc.edu

S. Barry Cooper

University of Leeds, School of Mathematics

Leeds LS2 9JT, UK

E-mail: s.b.cooper@leeds.ac.uk

Hong Zhu

Fudan University, Department of Computer Science and Engineering

220 Handan Road, Shanghai, 200433, China

E-mail: hzh@fudan.edu.cn

Library of Congress Control Number: 2007926619

CR Subject Classification (1998): F.1.1-2, F.2.1-2, F.4.1, I.2.6, J.3

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743

ISBN-10 3-540-72503-2 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-72503-9 Springer 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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 12063888 06/3180 5 4 3 2 1 0

Preface

Theory and Applications of Models of Computation (TAMC) is an international conference series with an interdisciplinary character, bringing together researchers working in computer science, mathematics (especially logic) and the physical sciences. This cross-disciplinary character, together with its focus on algorithms, complexity and computability theory, gives the conference a special flavor and distinction.

TAMC 2007 was the fourth conference in the series. The previous three meetings were held May 17 – 19, 2004 in Beijing, May 17 – 20, 2005 in Kunming, and May 15 – 20, 2006 in Beijing, P. R. China. TAMC 2007 was held in Shanghai, May 22 – 25, 2007. Future annual meetings are planned.

At TAMC 2007 we were very pleased to have two plenary speakers, Miklós Ajtai and Fan Chung Graham, each gave a one hour invited talk. Miklós Ajtai spoke on “Generalizations of the Compactness Theorem and Godel’s Completeness Theorem for Nonstandard Finite Structures,” and Fan Chung Graham spoke on “Detecting Sharp Drops in PageRank and a Simplified Local Partitioning Algorithm.” Their respective papers accompanying the talks are included in these proceedings.

In addition, there were two special sessions organized by Barry Cooper and Andrew Lewis on “Computability and Randomness” and by Manindra Agrawal and Angsheng Li on “Algorithms and Complexity.” The invited speakers included George Barmpalias, Cristian Calude, Bjorn Kjos-Hanssen, Andre Nies, and Jan Reimann in the “Computability and Randomness” special session, and Manindra Agrawal, Alberto Apostolico, Jin-Yi Cai, Andreas Dress, Naveen Garg and Jaikumar Radhakrishnan in the “Algorithms and Complexity” special session.

The TAMC conference series arose naturally in response to important scientific developments affecting how we compute in the twenty-first century. At the same time, TAMC is already playing an important regional and international role, and promises to become a key contributor to the scientific resurgence seen throughout China and other parts of Asia.

The enthusiasm with which TAMC 2007 was received by the scientific community is evident in the large number of quality articles submitted to the conference. There were over 500 submissions, originating from all over the world. This presented the Program Committee with a major assessment task. The Program Committee finally selected 67 papers for presentation at the conference and inclusion in this LNCS volume. This results in an acceptance rate of just over 13%, making TAMC an extremely selective conference, compared to other leading international conferences.

We are very grateful to the Program Committee, and the many outside referees they called on, for the hard work and expertise which they brought to

the difficult selection process. We also wish to thank all those authors who submitted their work for our consideration. The Program Committee could have accepted many more submissions without compromising standards, and were only restrained by the practicalities of scheduling so many talks, and by the inevitable limitations on the size of this proceedings volume.

Finally, we would like to thank the members of the Editorial Board of *Lecture Notes in Computer Science* and the Editors at Springer for their encouragement and cooperation throughout the preparation of this conference.

Of course TAMC 2007 would not have been possible without the support of our sponsors, and we therefore gratefully acknowledge their help in the realization of this conference.

May 2007

Jin-Yi Cai
S. Barry Cooper
Hong Zhu

Organization

The conference was organized by: the Software School of Fudan University; University of Leeds, UK; and the University of Wisconsin–Madison, USA.

Conference Chair

Jin-Yi Cai (University of Wisconsin)

Program Committee Co-chairs

S. Barry Cooper (University of Leeds)

Hong Zhu (Fudan University)

Program Committee

Giorgio Ausiello (University of Rome)

Eric Bach (University of Wisconsin)

Nicolò Cesa-Bianchi (University of Milan)

Jianer Chen (Texas A&M University)

Yijia Chen (Shanghai Jiaotong University)

Francis Chin (University of Hong Kong)

C.T. Chong (National University of Singapore)

Kyung-Yong Chwa (KAIST, Korea)

Decheng Ding (Nanjing University)

Rodney Downey (University of Wellington)

Martin Dyer (University of Leeds)

Rudolf Fleischer (Fudan University)

Oscar Ibarra (UC Santa Barbara)

Hiroshi Imai (University of Tokyo)

Kazuo Iwama (Kyoto University)

Tao Jiang (University of California-Riverside/Tsinghua)

Satyanaarayana Lokam (Microsoft Research-India)

D. T. Lee (Academia Sinica, Taipei)

Angsheng Li (Institute of Software, CAS, Beijing)

Giuseppe Longo (CNRS - Ecole Normale Supérieure, Paris)

Tian Liu (Peking University)

Rüdiger Reischuk (Universität zu Lübeck)

Rocco Servedio (Columbia University)

Alexander Shen (Institute for Information Transmission Problems, Moscow)

Yaoyun Shi (University of Michigan)

Theodore A. Slaman (UC Berkeley)

Xiaoming Sun (Tsinghua University)
Shanghua Teng (Boston University)
Luca Trevisan (UC Berkeley)
Christopher Umans (Cal Tech)
Alasdair Urquhart (University of Toronto)
Hanpin Wang (Peking University)
Osamu Watanabe (Tokyo Institute of Technology)
Zhiwei Xu (Institute of Computing Technology, CAS, Beijing)
Frances Yao (City University of Hong Kong)
Mingsheng Ying (Tsinghua University)

Organizing Committee

Jin-Yi Cai (The University of Wisconsin-Madison, USA)
S. Barry Cooper (University of Leeds, UK)
Angsheng Li (Institute of Software, Chinese Academy of Sciences, China)
Hong Zhu (Fudan University, China)

Sponsoring Institutions

The National Natural Science Foundation of China
Chinese Academy of Sciences
Microsoft Research, Asia
Science and Technology Commission of Shanghai Municipality
Software School of Fudan University

Table of Contents

Plenary Lectures

Detecting Sharp Drops in PageRank and a Simplified Local Partitioning Algorithm.....	1
<i>Reid Andersen and Fan Chung</i>	
Generalizations of the Compactness Theorem and Gödel's Completeness Theorem for Nonstandard Finite Structures	13
<i>Miklós Ajtai</i>	

Contributed Papers

Approximation Algorithms for 3D Orthogonal Knapsack	34
<i>Florian Diedrich, Rolf Harren, Klaus Jansen, Ralf Thöle, and Henning Thomas</i>	
A Comparative Study of Efficient Algorithms for Partitioning a Sequence into Monotone Subsequence	46
<i>Bing Yang, Jing Chen, Enyue Lu, and S.Q. Zheng</i>	
The Hardness of Selective Network Design for Bottleneck Routing Games.....	58
<i>Haiyang Hou and Guochuan Zhang</i>	
A Polynomial Time Algorithm for Finding Linear Interval Graph Patterns	67
<i>Hitoshi Yamasaki and Takayoshi Shoudai</i>	
Elementary Differences Among Jump Hierarchies	79
<i>Angsheng Li</i>	
Working with the <i>LR</i> Degrees	89
<i>George Barmpalias, Andrew E.M. Lewis, and Mariya Soskova</i>	
Computability on Subsets of Locally Compact Spaces	100
<i>Yatao Xu and Tanja Grubba</i>	
A New Approach to Graph Recognition and Applications to Distance-Hereditary Graphs	115
<i>Shin-ichi Nakano, Ryuhei Uehara, and Takeaki Uno</i>	
Finding a Duplicate and a Missing Item in a Stream	128
<i>Jun Tarui</i>	

Directed Searching Digraphs: Monotonicity and Complexity	136
<i>Boting Yang and Yi Cao</i>	
Protecting Against Key Escrow and Key Exposure in Identity-Based Cryptosystem	148
<i>Jin Wang, Xi Bai, Jia Yu, and Daxing Li</i>	
Encapsulated Scalar Multiplications and Line Functions in the Computation of Tate Pairing	159
<i>Rongquan Feng and Hongfeng Wu</i>	
A Provably Secure Blind Signature Scheme	171
<i>Xiaoming Hu and Shangteng Huang</i>	
Construct Public Key Encryption Scheme Using Ergodic Matrices over $GF(2)$	181
<i>Pei Shi-Hui, Zhao Yong-Zhe, and Zhao Hong-Wei</i>	
New Left-to-Right Radix-r Signed-Digit Recoding Algorithm for Pairing-Based Cryptosystems	189
<i>Fanyu Kong, Jia Yu, Zhun Cai, and Daxing Li</i>	
The Strongest Nonsplitting Theorem	199
<i>Mariya Ivanova Soskova and S. Barry Cooper</i>	
There is an Sw-Cupppable Strongly c.e. Real	212
<i>Yun Fan</i>	
On Computation Complexity of the Concurrently Enabled Transition Set Problem	222
<i>Li Pan, Weidong Zhao, Zhicheng Wang, Gang Wei, and Shumei Wang</i>	
Synchronization of Some DFA	234
<i>A.N. Trahtman</i>	
On the Treewidth and Pathwidth of Biconvex Bipartite Graphs	244
<i>Sheng-Lung Peng and Yi-Chuan Yang</i>	
On Exact Complexity of Subgraph Homeomorphism	256
<i>Andrzej Lingas and Martin Wahlen</i>	
Searching a Polygonal Region by Two Guards	262
<i>Xuehou Tan</i>	
On the Internal Steiner Tree Problem	274
<i>Sun-Yuan Hsieh, Huang-Ming Gao, and Shih-Cheng Yang</i>	
Approximately Optimal Trees for Group Key Management with Batch Updates	284
<i>Minming Li, Ze Feng, Ronald L. Graham, and Frances F. Yao</i>	

On Deciding Deep Holes of Reed-Solomon Codes	296
<i>Qi Cheng and Elizabeth Murray</i>	
Quantum Multiparty Communication Complexity and Circuit Lower Bounds	306
<i>Iordanis Kerenidis</i>	
Efficient Computation of Algebraic Immunity of Symmetric Boolean Functions	318
<i>Feng Liu and Keqin Feng</i>	
Improving the Average Delay of Sorting	330
<i>Andreas Jakoby, Maciej Liškiewicz, Rüdiger Reischuk, and Christian Schindelhauer</i>	
Approximating Capacitated Tree-Routings in Networks	342
<i>Ehab Morsy and Hiroshi Nagamochi</i>	
Feedback Arc Set Problem in Bipartite Tournaments	354
<i>Sushmita Gupta</i>	
Studying on Economic-Inspired Mechanisms for Routing and Forwarding in Wireless Ad Hoc Network	362
<i>Yufeng Wang, Yoshiaki Hori, and Kouichi Sakurai</i>	
Enhancing Simulation for Checking Language Containment	374
<i>Jin Yi and Wenhui Zhang</i>	
QBF-Based Symbolic Model Checking for Knowledge and Time	386
<i>Conghua Zhou, Zhenyu Chen, and Zhihong Tao</i>	
A Characterization of the Language Classes Learnable with Correction Queries	398
<i>Cristina Tîrnăuică and Satoshi Kobayashi</i>	
Learnable Algorithm on the Continuum	408
<i>Zhimin Li and Xiang Li</i>	
Online Deadline Scheduling with Bounded Energy Efficiency	416
<i>Joseph Wun-Tat Chan, Tak-Wah Lam, Kin-Sum Mak, and Prudence W.H. Wong</i>	
Efficient Algorithms for Airline Problem	428
<i>Shin-ichi Nakano, Ryuhei Uehara, and Takeaki Uno</i>	
Efficient Exact Arithmetic over Constructive Reals	440
<i>Yong Li and Jun-Hai Yong</i>	
Bounding Run-Times of Local Adiabatic Algorithms	450
<i>M.V. Panduranga Rao</i>	

A Note on Universal Composable Zero Knowledge in Common Reference String Model	462
<i>Andrew C.C. Yao, Frances F. Yao, and Yunlei Zhao</i>	
A Note on the Feasibility of Generalized Universal Composability	474
<i>Andrew C.C. Yao, Frances F. Yao, and Yunlei Zhao</i>	
t -Private and Secure Auctions	486
<i>Markus Hinkelmann, Andreas Jakoby, and Peer Stechert</i>	
Secure Multiparty Computations Using a Dial Lock	499
<i>Takaaki Mizuki, Yoshinori Kugimoto, and Hideaki Sone</i>	
A Time Hierarchy Theorem for Nondeterministic Cellular Automata ...	511
<i>Chuzo Iwamoto, Harumasa Yoneda, Kenichi Morita, and Katsunobu Imai</i>	
Decidability of Propositional Projection Temporal Logic with Infinite Models	521
<i>Zhenhua Duan and Cong Tian</i>	
Separation of Data Via Concurrently Determined Discriminant Functions	533
<i>Hong Seo Ryoo and Kwangsoo Kim</i>	
The Undecidability of the Generalized Collatz Problem	542
<i>Stuart A. Kurtz and Janos Simon</i>	
Combinatorial and Spectral Aspects of Nearest Neighbor Graphs in Doubling Dimensional and Nearly-Euclidean Spaces	554
<i>Yingchao Zhao and Shang-Hua Teng</i>	
Maximum Edge-Disjoint Paths Problem in Planar Graphs.....	566
<i>Mingji Xia</i>	
An Efficient Algorithm for Generating Colored Outerplanar Graphs	573
<i>Jiexun Wang, Liang Zhao, Hiroshi Nagamochi, and Tatsuya Akutsu</i>	
Orthogonal Drawings for Plane Graphs with Specified Face Areas	584
<i>Akifumi Kawaguchi and Hiroshi Nagamochi</i>	
Absolutely Non-effective Predicates and Functions in Computable Analysis	595
<i>Decheng Ding, Klaus Weihrauch, and Yongcheng Wu</i>	
Linear-Size Log-Depth Negation-Limited Inverter for k -Tonic Binary Sequences	605
<i>Hiroki Morizumi and Jun Tarui</i>	

The Existence of Unsatisfiable Formulas in k -LCNF for $k \geq 3$	616
<i>Qingshun Zhang and Daoyun Xu</i>	
Improved Exponential Time Lower Bound of Knapsack Problem Under BT Model.	624
<i>Xin Li, Tian Liu, Han Peng, Liyan Qian, Hongtao Sun, Jin Xu, Ke Xu, and Jiaqi Zhu</i>	
Phase Transition of Multivariate Polynomial Systems	632
<i>Giordano Fusco and Eric Bach</i>	
Approximation Algorithms for Maximum Edge Coloring Problem	646
<i>Wangsen Feng, Li'ang Zhang, Wanling Qu, and Hanpin Wang</i>	
Two Improved Range-Efficient Algorithms for F_0 Estimation	659
<i>He Sun and Chung Keung Poon</i>	
Approximation to the Minimum Rooted Star Cover Problem	670
<i>Wenbo Zhao and Peng Zhang</i>	
Approximability and Parameterized Complexity of Consecutive Ones Submatrix Problems.	680
<i>Michael Dom, Jiong Guo, and Rolf Niedermeier</i>	
Parameterized Algorithms for Weighted Matching and Packing Problems	692
<i>Yunlong Liu, Jianer Chen, and Jianxin Wang</i>	
Kernelizations for Parameterized Counting Problems	703
<i>Marc Thurley</i>	
Revisiting the Impossibility for Boosting Service Resilience	715
<i>Xingwu Liu, Zhiwei Xu, and Juhua Pu</i>	
An Approximation Algorithm to the k -Steiner Forest Problem	728
<i>Peng Zhang</i>	
A Distributed Algorithm of Fault Recovery for Stateful Failover	738
<i>Indranil Saha and Debapriyay Mukhopadhyay</i>	
Path Embedding on Folded Hypercubes.	750
<i>Sun-Yuan Hsieh</i>	
An Approximation Algorithm Based on Chain Implication for Constrained Minimum Vertex Covers in Bipartite Graphs	760
<i>Jianxin Wang, Xiaoshuang Xu, and Jianer Chen</i>	
Author Index	771