

*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*

Alfred Kobsa

*University of California, Irvine, CA, 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

*TU Dortmund University, Germany*

Madhu Sudan

*Microsoft Research, Cambridge, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbruecken, Germany*

Manindra Agrawal S. Barry Cooper  
Angsheng Li (Eds.)

# Theory and Applications of Models of Computation

9th Annual Conference, TAMC 2012  
Beijing, China, May 16-21, 2012  
Proceedings



Springer

## Volume Editors

Manindra Agrawal  
Indian Institute of Technology Kanpur  
Department of Computer Science and Engineering  
Resource Planning and Generation  
208016 Kanpur, India  
E-mail: manindra@iitk.ac.in

S. Barry Cooper  
University of Leeds  
Department of Pure Mathematics  
Leeds LS2 9JT, UK  
E-mail: pmt6sbc@amsta.leeds.ac.uk

Angsheng Li  
Chinese Academy of Sciences  
Institute of Software  
P.O. Box 8718  
Beijing, 100190, P.R. China  
E-mail: angsheng@ios.ac.cn

ISSN 0302-9743  
ISBN 978-3-642-29951-3  
DOI 10.1007/978-3-642-29952-0  
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349  
e-ISBN 978-3-642-29952-0

Library of Congress Control Number: 2012936254

CR Subject Classification (1998): F.2, F.3, F.4, G.2.2, H.1.1, E.1, G.4, I.1

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

© Springer-Verlag Berlin Heidelberg 2012

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

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

Printed on acid-free paper

Springer is part of Springer Science+Business Media ([www.springer.com](http://www.springer.com))

# 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 and the physical sciences. It is this, together with its predominantly computational and computability theoretic focus, which gives the series its special character.

TAMC 2012 was the ninth conference in the series, organized as a Turing Centenary Meeting. The conference was combined with the Turing Lectures 2012, dedicated to celebrating Alan Turing's unique impact on mathematics, computing, computer science, informatics, morphogenesis, philosophy and the wider scientific world. Eight Turing Lectures were given at TAMC 2012 and the Turing Year in China.

Turing Lectures 2012:

- S. Barry Cooper (Leeds), *From Turing Machine to Morphogenesis – Forming and Informing Computation*
- John Hopcroft (Cornell), *On the Impact of Turing Machines*
- Richard Karp (Berkeley), *Theory of Computation as an Enabling Tool for the Sciences*
- Jon Kleinberg (Cornell), *The Convergence of Social and Technological Networks*
- Butler Lampson (Microsoft), *What Computers Do: Model, Connect, Engage*
- Deyi Li (CAE, China), *Interaction and Collective Intelligence on the Internet*
- Wei Li (BUAA, Beijing), *R-Calculus: A Logical Inference System for Scientific Discovery*
- Andrew C. Yao (Tsinghua University, Beijing), *Quantum Computing: A Great Science in the Making.*

There were four special sessions at TAMC 2012, each with an Organizing Chair, and some invited speakers to give talks in corresponding fields. These were:

- Algorithms and Information in Networks. Organized by Zhiyong Liu (ICT, CAS) with speakers: Antonio Fernandez (Institute IMDEA Networks, Spain), Albert Frederick Lawrence (University of California San Diego, School of Medicine), Yicheng Pan (Institute of Software, Chinese Academy of Sciences), and Xiaoming Sun (Institute of Computing Technology, Chinese Academy of Sciences).
- Complexity and Cryptography. Organized by Xiaotie Deng (HK), with speakers: Xi Chen (Columbia University), Ning Chen (Singapore, NTU), and Yi Deng (ISCAS).
- Models of Computing and Networking. Organized by Anthony Bonato with speakers: Anthony Bonato (Ryerson University), Jure Leskovec (Stanford University), and Pan Peng (ISCAS).

- Programming and Verification. Organized by Wenhui Zhang (ISCAS), with speakers: Xinyu Feng (University of Science and Technology, China), Deepak Kapur (University of New Mexico, USA), Ernst-Ruediger Olderog (University of Oldenburg, Germany), and Naijun Zhan (Institute of Software, Chinese Academy of Sciences, China).

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 the Asia-Pacific region.

There were 86 quality submissions to TAMC 2012, originating from 27 countries, from which the Program Committee selected 40 excellent papers for inclusion in this LNCS volume. Together with the papers from the invited special session speakers and from the Turing Lecturers, this makes the current volume special and valuable.

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.

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.

Both the Turing Lectures 2012 and TAMC 2012 would not have been possible without the support of our sponsors: State Key Laboratory of Computer Science (China), Institute of Software (Chinese Academy of Sciences), and Chinese Academy of Sciences, and we therefore gratefully acknowledge their help in the realization of this special Turing Centenary conference.

March 2012

Manindra Agrawal  
Barry Cooper  
Angsheng Li

# Organization

The conference was organized by the State Key Laboratory of Computer Science, and Institute of Software, Chinese Academy of Sciences.

## Program Committee

Manindra Agrawal	IIT at Kanpur, India (Co-chair)
Marat Arslanov	Kazan University, Russia
Giorgio Ausiello	Dresden University, Germany
George Barmpalias	Institute of Software, Chinese Academy of Sciences, China
Anthony Bonato	Ryerson University, Canada
Christian Calude	University of Auckland, New Zealand
Alessandra Carbone	Université Pierre et Marie Curie, France
Jianer Chen	Texas A&M, USA
Wei Chen	Microsoft Research Asia
Francis Y.L. Chin	University of Hong Kong, SAR China
S. Barry Cooper	University of Leeds, UK (Co-chair)
Luca Cardelli	Cambridge University, UK
Gilles Dowek	INRIA, Paris, France
Zhenhua Duan	Xidian University, China
Mike Fellows	Charles Darwin University, Australia
Kazuo Iwama	Kyoto University, Japan
Andrew Lewis	University of Leeds, UK
Angsheng Li	Institute of Software, Chinese Academy of Sciences, China (Co-chair)
Weiyi Liu	Yunnan University, China
Zhiyong Liu	Institute of Computing Technology, Chinese Academy of Sciences, China
Giuseppe Longo	École Normale Supérieure, France
Mitsunori Ogiwara	University of Miami, USA
Luke Ong	University of Oxford, UK
Xiaoming Sun	Tsinghua University, China
Yongji Wang	Institute of Software, Chinese Academy of Sciences, China
Osamu Watanabe	Tokyo Institute of Technology, Japan
Peng Zhang	Shandong University, China
Naijun Zhan	Institute of Software, Chinese Academy of Sciences, China
Ting Zhang	Iowa State University, USA

## Steering Committee

Manindra Agrawal	IIT at Kanpur, India
Jin-Yi Cai	University of Wisconsin-Madison, USA
S. Barry Cooper	University of Leeds, UK
John Hopcroft	Cornell University, USA
Angsheng Li	Institute of Software, Chinese Academy of Sciences, China (Chair)

## Local Organizing Committee

George Barmpalias (ISCAS)  
Yunfu Cao (ISCAS)  
Haiming Chen (ISCAS)  
Zhiming Ding (ISCAS)  
Angsheng Li (ISCAS, Co-chair)  
Yucheng Li (ISCAS, Co-chair)  
Dongdai Lin (ISCAS)  
Kelong Liu (ISCAS)  
Hongan Wang (ISCAS)  
Mingji Xia (ISCAS)  
Ye Yang (ISCAS)  
Yongji Wang (ISCAS)  
Naijun Zhan (ISCAS)

## Organizing Committee for the Turing Year in China

George Barmpalias (ISCAS)  
S. Barry Cooper (Leeds)  
John Hopcroft (Cornell)  
Angsheng Li (ISCAS, Co-chair)  
Yucheng Li (ISCAS, Co-chair)  
Huimin Lin (ISCAS)  
Pengzhi Liu (Renmin High School, Co-chair)  
Zhiyong Liu (ICT, CAS)  
Ruqian Lu (Math Academy, CAS)  
Jian Zhang (ISCAS)  
Chaochen Zhou (ISCAS)

## **Local Organizing Committee for the Turing Year in China**

George Barmpalias (ISCAS)  
Yunfu Cao (ISCAS)  
Haiming Chen (ISCAS)  
Zhiming Ding (ISCAS)  
Angsheng Li (ISCAS, Co-chair)  
Yucheng Li (ISCAS, Co-chair)  
Dongdai Lin (ISCAS)

## **Sponsoring Institutions**

State Key Laboratory of Computer Science  
Institute of Software, Chinese Academy of Sciences  
Chinese Academy of Sciences



# Table of Contents

## Turing Lectures 2012

On the Impact of Turing Machines . . . . .	1
<i>John Hopcroft</i>	
From Turing Machine to Morphogenesis: Forming and Informing Computation . . . . .	3
<i>S. Barry Cooper</i>	
Theory of Computation as an Enabling Tool for the Sciences . . . . .	11
<i>Richard M. Karp</i>	
Interaction and Collective Intelligence on the Internet . . . . .	12
<i>Deyi Li and Liwei Huang</i>	
What Computers Do: Model, Connect, Engage . . . . .	23
<i>Butler Lampson</i>	
R-Calculus: A Logical Inference System for Scientific Discovery . . . . .	27
<i>Wei Li</i>	
Quantum Computing: A Great Science in the Making . . . . .	28
<i>Andrew Chi-Chih Yao</i>	
The Convergence of Social and Technological Networks . . . . .	29
<i>Jon Kleinberg</i>	

## Invited Lectures

Principles of Network Computing . . . . .	30
<i>Yicheng Pan</i>	
The Small Community Phenomenon in Networks: Models, Algorithms and Applications . . . . .	40
<i>Pan Peng</i>	
Vertex-Pursuit in Hierarchical Social Networks . . . . .	50
<i>A. Bonato, D. Mitsche, and P. Pralat</i>	
A Structural Approach to Prophecy Variables . . . . .	61
<i>Zipeng Zhang, Xinyu Feng, Ming Fu, Zhong Shao, and Yong Li</i>	
An Assume/Guarantee Based Compositional Calculus for Hybrid CSP . . . . .	72
<i>Shuling Wang, Naijun Zhan, and Dimitar Guelev</i>	

Automatic Verification of Real-Time Systems with Rich Data: An Overview .....	84
<i>Ernst-Rüdiger Olderog</i>	
Program Analysis Using Quantifier-Elimination Heuristics (Extended Abstract) .....	94
<i>Deepak Kapur</i>	
Electron Tomography and Multiscale Biology .....	109
<i>Albert F. Lawrence, Séastien Phan, and Mark Ellisman</i>	

## Contributed Papers

Constant-Time Approximation Algorithms for the Knapsack Problem .....	131
<i>Hiro Ito, Susumu Kiyoshima, and Yuichi Yoshida</i>	
Lower Bounds of Shortest Vector Lengths in Random NTRU Lattices .....	143
<i>Jingguo Bi and Qi Cheng</i>	
Polynomial Time Construction of Ellipsoidal Approximations of Zonotopes Given by Generator Descriptions .....	156
<i>Michal Černý and Miroslav Rada</i>	
Hardness and Approximation of the Asynchronous Border Minimization Problem (Extended Abstract) .....	164
<i>Alexandru Popa, Prudence W.H. Wong, and Fencol C.C. Yung</i>	
Asymptotic Limits of a New Type of Maximization Recurrence with an Application to Bioinformatics .....	177
<i>Kun-Mao Chao, An-Chiang Chu, Jesper Jansson, Richard S. Lemence, and Alban Mancheron</i>	
Computing Bits of Algebraic Numbers .....	189
<i>Samir Datta and Rameshwar Pratap</i>	
Approximating MAX SAT by Moderately Exponential and Parameterized Algorithms .....	202
<i>Bruno Escoffier, Vangelis Th. Paschos, and Emeric Tourniaire</i>	
Computing Error Distance of Reed-Solomon Codes .....	214
<i>Guizhen Zhu and Daqing Wan</i>	
Coordination Mechanisms for Selfish Parallel Jobs Scheduling (Extended Abstract) .....	225
<i>Deshi Ye and Guochuan Zhang</i>	

Computationally-Fair Group and Identity-Based Key-Exchange . . . . .	237
<i>Andrew C. Yao and Yunlei Zhao</i>	
Timed Encryption with Application to Deniable Key Exchange . . . . .	248
<i>Shaoquan Jiang</i>	
Online Makespan Scheduling of Linear Deteriorating Jobs on Parallel Machines (Extended Abstract) . . . . .	260
<i>Sheng Yu, Jude-Thaddeus Ojiaku, Prudence W.H. Wong, and Yinfeng Xu</i>	
A Surprisingly Simple Way of Reversing Trace Distance via Entanglement . . . . .	273
<i>Jun Yan</i>	
Constructions for Binary Codes Correcting Asymmetric Errors from Function Fields . . . . .	284
<i>Jun Zhang and Fang-Wei Fu</i>	
Stopping Set Distributions of Algebraic Geometry Codes from Elliptic Curves . . . . .	295
<i>Jun Zhang, Fang-Wei Fu, and Daqing Wan</i>	
Energy-Efficient Network Routing with Discrete Cost Functions . . . . .	307
<i>Lin Wang, Antonio Fernández Anta, Fa Zhang, Chenying Hou, and Zhiyong Liu</i>	
An Algorithmic View on Multi-Related-Segments: A Unifying Model for Approximate Common Interval . . . . .	319
<i>Xiao Yang, Florian Sikora, Guillaume Blin, Sylvie Hamel, Romeo Rizzi, and Srinivas Aluru</i>	
The Worst Case Behavior of Randomized Gossip . . . . .	330
<i>H. Baumann, P. Fraigniaud, H.A. Harutyunyan, and R. de Verclos</i>	
Holographic Algorithms on Domain Size $k > 2$ . . . . .	346
<i>Zhiguo Fu and Jin-Yi Cai</i>	
A Refined Exact Algorithm for Edge Dominating Set . . . . .	360
<i>Mingyu Xiao and Hiroshi Nagamochi</i>	
Finite Automata over Structures (Extended Abstract) . . . . .	373
<i>Aniruddh Gandhi, Bakhtadyr Khoussainov, and Jiamou Liu</i>	
Deterministic Distributed Data Aggregation under the SINR Model . . .	385
<i>Nathaniel Hobbs, Yuxuan Wang, Qiang-Sheng Hua, Dongxiao Yu, and Francis C.M. Lau</i>	

Tensor Rank and Strong Quantum Nondeterminism in Multiparty Communication .....	400
<i>Marcos Villagra, Masaki Nakanishi, Shigeru Yamashita, and Yasuhiko Nakashima</i>	
Speed Scaling Problems with Memory/Cache Consideration .....	412
<i>Weiwei Wu, Minming Li, He Huang, and Enhong Chen</i>	
On the Amount of Nonconstructivity in Learning Formal Languages from Positive Data .....	423
<i>Sanjay Jain, Frank Stephan, and Thomas Zeugmann</i>	
Computing in the Fractal Cloud: Modular Generic Solvers for SAT and Q-SAT Variants .....	435
<i>Denys Duchier, Jérôme Durand-Lose, and Maxime Senot</i>	
Online Optimization of Busy Time on Parallel Machines (Extended Abstract) .....	448
<i>Mordechai Shalom, Ariella Voloshin, Prudence W.H. Wong, Fencol C.C. Yung, and Shmuel Zaks</i>	
Bisection (Band)Width of Product Networks with Application to Data Centers .....	461
<i>Jordi Arjona Aroca and Antonio Fernández Anta</i>	
Implicit Computation of Maximum Bipartite Matchings by Sublinear Functional Operations .....	473
<i>Beate Bollig, Marc Gillé, and Tobias Pröger</i>	
A Game-Theoretic Approach for Balancing the Tradeoffs between Data Availability and Query Delay in Multi-hop Cellular Networks .....	487
<i>Jin Li, Weiyi Liu, and Kun Yue</i>	
Proving Liveness Property under Strengthened Compassion Requirements .....	498
<i>Teng Long and Wenhui Zhang</i>	
Realizing Monads in Interaction Nets via Generic Typed Rules .....	509
<i>Eugen Jiresch and Bernhard Gramlich</i>	
Towards an Axiomatization of Simple Analog Algorithms .....	525
<i>Olivier Bournez, Nachum Dershowitz, and Evgenia Falkovich</i>	
Multiple Usage of Random Bits in Finite Automata .....	537
<i>Rūsiņš Freivalds</i>	
Minimum Certificate Dispersal with Tree Structures .....	548
<i>Taisuke Izumi, Tomoko Izumi, Hirotaka Ono, and Koichi Wada</i>	

Improved FPT Algorithms for Rectilinear $k$ -Links Spanning Path . . . . .	560
<i>Jianxin Wang, Jinyi Yao, Qilong Feng, and Jianer Chen</i>	
FPT Results for Signed Domination . . . . .	572
<i>Ying Zheng, Jianxin Wang, Qilong Feng, and Jianer Chen</i>	
Submodular Minimization via Pathwidth . . . . .	584
<i>Hiroshi Nagamochi</i>	
A Detailed Study of the Dominating Cliques Phase Transition in Random Graphs . . . . .	594
<i>Martin Nehéz, Daniel Olejár, and Michal Demetrian</i>	
An Application of 1-Genericity in the $\Pi_2^0$ Enumeration Degrees . . . . .	604
<i>Liliana Badillo and Charles M. Harris</i>	
<b>Author Index</b> . . . . .	621