

*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*

Susanne Graf Wenhui Zhang (Eds.)

# Automated Technology for Verification and Analysis

4th International Symposium, ATVA 2006  
Beijing, China, October 23-26, 2006  
Proceedings

Volume Editors

Susanne Graf  
VERIMAG  
Centre Equation - 2, Avenue de Vignate  
F-38610 Gieres, France  
E-mail: Susanne.Graf@imag.fr

Wenhui Zhang  
Chinese Academy of Sciences  
Institute of Software  
P.O. Box 8718, Beijing, China  
E-mail: zwh@ios.ac.cn

Library of Congress Control Number: 2006934115

CR Subject Classification (1998): B.1.2, B.5.2, B.6, B.7.2, C.2, C.3, D.2, D.3, F.3

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN           0302-9743  
ISBN-10       3-540-47237-1 Springer Berlin Heidelberg New York  
ISBN-13       978-3-540-47237-7 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 2006  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper      SPIN: 11901914      06/3142      5 4 3 2 1 0

# Preface

The Automated Technology for Verification and Analysis (ATVA) international symposium series was initiated in 2003, responding to a growing interest in formal verification spurred by the booming IT industry, particularly hardware design and manufacturing in East Asia. Its purpose is to promote research on automated verification and analysis in the region by providing a forum for interaction between the regional and the international research/industrial communities of the field. ATVA 2006, the fourth of the ATVA series, was held in Beijing, China, October 23-26, 2006. The main topics of the symposium include theories useful for providing designers with automated support for obtaining correct software or hardware systems, as well as the implementation of such theories in tools or their application.

This year, we received a record number of papers: a total of 137 submissions from 27 countries. Each submission was assigned to three Program Committee members, who could request help from subreviewers, for rigorous and fair evaluation. The final deliberation by the Program Committee was conducted through Springer's Online Conference Service for a duration of about 10 days after nearly all review reports had been collected. In the end, 35 papers were selected for inclusion in the program.

ATVA 2006 had three keynote speeches given respectively by Thomas Ball, Jin Yang, and Mihalis Yannakakis. The main symposium was preceded by a tutorial day, consisting of three two-hour lectures given by the keynote speakers.

ATVA 2006 was supported by the National Natural Science Foundation of China and the Institute of Software of the Chinese Academy of Sciences. Their generous sponsorships are gratefully acknowledged. We would like to thank the Program Committee members and their subreviewers for their hard work in evaluating the submissions and selecting the program. We thank the keynote speakers for their extra effort in delivering the tutorials. We thank the Steering Committee for their advice, particularly Farn Wang, who also served as program chair of the first two ATVA symposia, for providing valuable suggestions.

For the administrative support, we thank the Laboratory of Computer Science at the Institute of Software of the Chinese Academy of Sciences. We also thank Martin Karusseit from Metaframe for his help with the online conference server.

October 2006

Susanne Graf  
Wenhui Zhang

# Organization

## Steering Committee

E. Allen Emerson	University of Texas at Austin
Oscar H. Ibarra	University of California at Santa Barbara
Insup Lee	University of Pennsylvania
Doron A. Peled	University of Warwick
Farn Wang	National Taiwan University
Hsu-Chun Yen	National Taiwan University

## General Chair

Huimin Lin	Chinese Academy of Sciences
------------	-----------------------------

## Sponsoring Organizations

National Natural Science Foundation of China  
Institute of Software of the Chinese Academy of Sciences

## Program Committee

Rajeev Alur	University of Pennsylvania
Christel Baier	University of Bonn
Jonathan Billington	University of South Australia
Sung-Deok Cha	Korea Advanced Inst. of Sci. and Techn.
Shing-Chi Cheung	Hong Kong Univ. of Sci. and Techn.
Ching-Tsun Chou	Intel
Jin Song Dong	National University of Singapore
E. Allen Emerson	University of Texas at Austin
Masahiro Fujita	University of Tokyo
Susanne Graf	VERIMAG
Wolfgang Grieskamp	Microsoft research
Teruo Higashino	Osaka University
Pei-Hsin Ho	Synopsys
Oscar H. Ibarra	University of California at Santa Barbara
Orna Kupferman	Hebrew University
Robert P. Kurshan	Cadence
Insup Lee	University of Pennsylvania
Xuandong Li	Nanjing University

Shaoying Liu	Hosei University
Zhiming Liu	IIST/United Nations University
Mila E. Majster-Cederbaum	University of Mannheim
Olaf Owe	University of Oslo
Doron A. Peled	University of Warwick
Zhong Shao	Yale University
Xiaoyu Song	Portland State University
Yih-Kuen Tsay	National Taiwan University
Irek Ulidowski	Leicester University
Bow-Yaw Wang	Academia Sinica
Farn Wang	National Taiwan University
Ji Wang	National U. of Techn. of China
Yi Wang	Uppsala University
Baowen Xu	Southeast University of China
Hsu-Chun Yen	National Taiwan University
Tomohiro Yoneda	Tokyo Institute of Technology
Wenhui Zhang	Chinese Academy of Sciences
Lenore Zuck	University of Illinois at Chicago

## Local Organization Chair

Naijun Zhan Chinese Academy of Sciences

## Reviewers

Hasan Amjad	Zhenbang Chen	Vijay Gehlot
Madhukar Anand	Zhenyu Chen	Stephen Gorton
Dave Arney	Chih-Hong Cheng	Zonghua Gu
Louise Avila	Rance Cleaveland	Arie Gurfinkel
Ittai Balaban	Gavin Cox	Ping Hao
Frederic Beal	Zhe Dang	Chris Hawblitzel
Ritwik Bhattacharya	Stephane Demri	Holger Hermanns
Howard Bowman	Yuxin Deng	Geng-Dian Huang
Marius Bozga	Jyotirmoy Deshmukh	Samuel Hym
Victor Braberman	Johan Dovland	John Håkansson
Thomas Brihaye	Claude Dutheillet	Mengluo Ji
Lin-Zan Cai	Karsten Ehrig	Li Jiao
Meeyoung Cha	Edith Elkind	Einar Broch Johnsen
Wen-Chin Chan	Colin Fidge	Ferhat Khendek
Chien-Liang Chen	Sebastian Fischmeister	Taeho Kim
Chunqing Chen	Joern Freiheit	Piotr Kosiuczenko
Liqian Chen	Felix Freiling	Maciej Koutny
Xiaofang Chen	Xiang Fu	Lars Kristensen
Yu-Fang Chen	Guy Gallasch	Sava Krstic

Georgios Lajios  
 Charles Lakos  
 François Laroussinie  
 Heungkyu Lee  
 Wenjun Lee  
 Tim Leonard  
 Guangyuan Li  
 Wenjun Li  
 Nimrod Lilith  
 Yih-Kai Lin  
 Zhi-Wei Lin  
 Lin Liu  
 Wanwei Liu  
 Yang Liu  
 Alessio Lomuscio  
 Bozena Wozna  
 Jih-Shien Lu  
 Yi Lu  
 Michael Luttenberger  
 Chamnika Mannakkara  
 Moritz Martens  
 Michael May  
 Christoph Minnameier  
 Anders Moen  
 Armaghan Naik

Akio Nakata  
 Dinesh Nikhil  
 Carl I. Colombo Nilsen  
 Kozo Okano  
 Peter Ølveczky  
 Rotem Oshman  
 Joel Ouaknine  
 Chun Ouyang  
 Robert Palmer  
 Jun Pang  
 Bo-Yuan Peng  
 Paul Petterson  
 Nir Piterman  
 Amir Pnueli  
 Zdenek Sawa  
 Sven Schewe  
 Tzay-Farn Shih  
 Jeremy Sproston  
 Volker Stolz  
 Jun Sun  
 Jinsong Tan  
 Arild Torjusen  
 Gerardo Schneider  
 Ralf Treinen  
 Ming-Hsien Tsai

Emilio Tuosto  
 Somsak Vanit-Anunchai  
 Thomas Wahl  
 Jun Wei  
 Verena Wolf  
 Bozena Wozna  
 Baohua Wu  
 Kang-Nien Wu  
 Ke-Ren Wu  
 Gaoyan Xie  
 Chang Xu  
 Jin Yang  
 Tuba Yavuz-Khaveci  
 Chunyang Ye  
 Xiaodong Yi  
 Hong Qing Yu  
 Ingrid Chieh Yu  
 Lien-Po Yu  
 Naijun Zhan  
 Tian Zhang  
 Jianhua Zhao  
 Liang Zhao  
 Conghua Zhou  
 Xiaocong Zhou

# Table of Contents

## Keynote Speeches

Analysis of Recursive Probabilistic Models . . . . .	1
<i>Mihalis Yannakakis</i>	
Verification Challenges and Opportunities in the New Era of Microprocessor Design . . . . .	6
<i>Jin Yang</i>	
Automated Abstraction of Software . . . . .	8
<i>Thomas Ball</i>	

## Regular Papers

Symmetry Reduction for Probabilistic Model Checking Using Generic Representatives . . . . .	9
<i>Alastair F. Donaldson, Alice Miller</i>	
Eager Markov Chains . . . . .	24
<i>Parosh Aziz Abdulla, Noomene Ben Henda, Richard Mayr, Sven Sandberg</i>	
A Probabilistic Learning Approach for Counterexample Guided Abstraction Refinement . . . . .	39
<i>Fei He, Xiaoyu Song, Ming Gu, Jiaguang Sun</i>	
A Fine-Grained Fullness-Guided Chaining Heuristic for Symbolic Reachability Analysis . . . . .	51
<i>Ming-Ying Chung, Gianfranco Ciardo, Andy Jingqing Yu</i>	
Model Checking Timed Systems with Urgencies . . . . .	67
<i>Pao-Ann Hsiung, Shang-Wei Lin, Yean-Ru Chen, Chun-Hsian Huang, Jia-Jen Yeh, Hong-Yu Sun, Chao-Sheng Lin, Hsiao-Win Liao</i>	
Whodunit? Causal Analysis for Counterexamples . . . . .	82
<i>Chao Wang, Zijiang Yang, Franjo Ivančić, Aarti Gupta</i>	



On the Membership Problem for Visibly Pushdown Languages . . . . .	96
<i>Salvatore La Torre, Margherita Napoli, Mimmo Parente</i>	
On the Construction of Fine Automata for Safety Properties . . . . .	110
<i>Orna Kupferman, Robby Lampert</i>	
On the Succinctness of Nondeterminism . . . . .	125
<i>Benjamin Aminof, Orna Kupferman</i>	
Efficient Algorithms for Alternating Pushdown Systems with an Application to the Computation of Certificate Chains . . . . .	141
<i>Dejvuth Suwimonteerabuth, Stefan Schwoon, Javier Esparza</i>	
Compositional Reasoning for Hardware/Software Co-verification . . . . .	154
<i>Fei Xie, Guowu Yang, Xiaoyu Song</i>	
Learning-Based Symbolic Assume-Guarantee Reasoning with Automatic Decomposition . . . . .	170
<i>Wonhong Nam, Rajeev Alur</i>	
On the Satisfiability of Modular Arithmetic Formulae . . . . .	186
<i>Bow-Yaw Wang</i>	
Selective Approaches for Solving Weak Games . . . . .	200
<i>Malte Helmert, Robert Mattmüller, Sven Schewe</i>	
Controller Synthesis and Ordinal Automata . . . . .	215
<i>Thierry Cachat</i>	
Effective Contraction of Timed STGs for Decomposition Based Timed Circuit Synthesis . . . . .	229
<i>Tomohiro Yoneda, Chris J. Myers</i>	
Synthesis for Probabilistic Environments . . . . .	245
<i>Sven Schewe</i>	
Branching-Time Property Preservation Between Real-Time Systems . . . . .	260
<i>Jinfeng Huang, Marc Geilen, Jeroen Voeten, Henk Corporaal</i>	
Automatic Verification of Hybrid Systems with Large Discrete State Space . . . . .	276
<i>Werner Damm, Stefan Disch, Hardi Hungar, Jun Pang, Florian Pigorsch, Christoph Scholl, Uwe Waldmann, Boris Wirtz</i>	
Timed Unfoldings for Networks of Timed Automata . . . . .	292
<i>Patricia Bouyer, Serge Haddad, Pierre-Alain Reynier</i>	

Symbolic Unfoldings for Networks of Timed Automata . . . . .	307
<i>Franck Cassez, Thomas Chatain, Claude Jard</i>	
Ranked Predicate Abstraction for Branching Time: Complete, Incremental, and Precise . . . . .	322
<i>Harald Fecher, Michael Huth</i>	
Timed Temporal Logics for Abstracting Transient States . . . . .	337
<i>Houda Bel Mokadem, Béatrice Bérard, Patricia Bouyer, François Laroussinie</i>	
Predicate Abstraction of Programs with Non-linear Computation . . . . .	352
<i>Songtao Xia, Ben Di Vito, Cesar Munoz</i>	
A Fresh Look at Testing for Asynchronous Communication . . . . .	369
<i>Puneet Bhateja, Paul Gastin, Madhavan Mukund</i>	
Proactive Leader Election in Asynchronous Shared Memory Systems . . . .	384
<i>M.C. Dharmadeep, K. Gopinath</i>	
A Semantic Framework for Test Coverage . . . . .	399
<i>Laura Brandán Briones, Ed Brinksma, Mariëlle Stoelinga</i>	
Monotonic Set-Extended Prefix Rewriting and Verification of Recursive Ping-Pong Protocols . . . . .	415
<i>Giorgio Delzanno, Javier Esparza, Jiří Srba</i>	
Analyzing Security Protocols in Hierarchical Networks . . . . .	430
<i>Ye Zhang, Hanne Riis Nielson</i>	
Functional Analysis of a Real-Time Protocol for Networked Control Systems . . . . .	446
<i>Colin Fidge, Yu-Chu Tian</i>	
Symbolic Semantics for the Verification of Security Properties of Mobile Petri Nets . . . . .	461
<i>Fernando Rosa-Velardo, David de Frutos-Escrig</i>	
Sigref – A Symbolic Bisimulation Tool Box . . . . .	477
<i>Ralf Wimmer, Marc Herbstritt, Holger Hermanns, Kelley Strampp, Bernd Becker</i>	
Towards a Model-Checker for Counter Systems . . . . .	493
<i>Stephane Demri, Alain Finkel, Valentin Goranko, Govert van Drimmelen</i>	

The Implementation of Mazurkiewicz Traces in POEM ..... 508  
*Peter Niebert, Hongyang Qu*

Model-Based Tool-Chain Infrastructure for Automated Analysis  
of Embedded Systems ..... 523  
*Hang Su, Graham Hemingway, Kai Chen, T. John Koo*

**Author Index** ..... 539