

*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

*New York University, NY, 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*

Farn Wang (Ed.)

# Automated Technology for Verification and Analysis

Second International Conference, ATVA 2004  
Taipei, Taiwan, ROC, October 31–November 3, 2004  
Proceedings



Springer

Volume Editor

Farn Wang  
National Taiwan University  
Department of Electrical Engineering  
1, Sec. 4, Roosevelt Rd., Taipei, Taiwan 106, ROC  
E-mail: farn@cc.ee.ntu.edu.tw

Library of Congress Control Number: 2004113833

CR Subject Classification (1998): B.1.2, B.2.2, B.5.2, B.6, B.7.2, C.2, C.3, D.2, D.3, F.3

ISSN 0302-9743

ISBN 3-540-23610-4 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

[springeronline.com](http://springeronline.com)

© Springer-Verlag Berlin Heidelberg 2004  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH  
Printed on acid-free paper SPIN: 11339656 06/3142 5 4 3 2 1 0

# Preface

It was our great pleasure to hold the 2nd International Symposium on Automated Technology on Verification and Analysis (ATVA) in Taipei, Taiwan, ROC, October 31–November 3, 2004. The series of ATVA meetings is intended for the promotion of related research in eastern Asia. In the last decade, automated technology on verification has become the new strength in industry and brought forward various hot research activities in both Europe and USA. In comparison, eastern Asia has been quiet in the forum. With more and more IC design houses moving from Silicon Valley to eastern Asia, we believe this is a good time to start cultivating related research activities in the region.

The emphasis of the ATVA workshop series is on various mechanical and informative techniques, which can give engineers valuable feedback to fast converge their designs according to the specifications. The scope of interest contains the following research areas: model-checking theory, theorem-proving theory, state-space reduction techniques, languages in automated verification, parametric analysis, optimization, formal performance analysis, real-time systems, embedded systems, infinite-state systems, Petri nets, UML, synthesis, tools, and practice in industry.

As a young symposium, ATVA 2004 succeeded in attracting 69 submissions from all over the world. All submissions were rigorously reviewed by three reviewers and discussed by the PC members through the network. The final program included a general symposium and three special tracks: (1) Design of secure/high-reliability networks, (2) HW/SW coverification and cosynthesis, and (3) hardware verification. The general symposium consisted of 24 regular papers and 8 short papers. The three special tracks together accepted 7 papers. The final program also included three keynote speeches by Bob Kurshan, Rajeev Alur, and Pei-Hsin Ho; and three invited speeches by Jean-Pierre Jouannaud, Tevfik Bultan, and Shaoying Liu. The symposium was also preceded by three tutorials by Bob Kurshan, Rajeev Alur, and Pei-Hsin Ho.

We want to thank the National Science Council, Ministry of Education, and Academia Sinica of Taiwan, ROC. Without their support, ATVA 2004 would not have come to reality. We thank the Department of Electrical Engineering, Center for Information and Electronics Technologies (CIET), SOC Center, and Graduate Institute of Electronic Engineering (GIEE) of National Taiwan University for their sturdy support, and we thank Synopsys, Inc. for sponsoring ATVA 2004. We thank all the tutorial–keynote speakers, invited speakers, committee members, and reviewers of ATVA 2004. Finally, we thank Mr. Rong-Shiung Wu, for his help in maintaining the webpages and compiling the proceedings, and Mr. Lin-Zan Cai, for his help in all the paperwork.

# Organization

## Steering Committee

E.A. Emerson (USA) Oscar H. Ibarra (USA)  
Insup Lee (USA) Doron A. Peled (UK)  
Farn Wang (Taiwan) Hsu-Chun Yen (Taiwan)

## Organizing Chair

Hsu-Chun Yen

## Program Chair

Farn Wang

## Program Committee

Tommaso Bolognesi (Italy)	Tevfik Bultan (USA)
Sungdeok Cha (Korea)	Yung-Ping Cheng (Taiwan)
Jin-Young Choi (Korea)	Jing-Song Dong (Singapore)
Jifeng He (China)	Teruo Higashino (Japan)
Pao-Ann Hsiung (Taiwan)	Chung-Yang Huang (Taiwan)
Oscar H. Ibarra (USA)	Insup Lee (USA)
Huimin Lin (China)	Doron A. Peled (UK)
Scott D. Stoller (USA)	Yih-Kuen Tsay (Taiwan)
Bow-Yaw Wang (Taiwan)	Farn Wang (Taiwan)
Hsu-Chun Yen (Taiwan)	Tomohiro Yoneda (Japan)

## Special Tracks

1. Design of Secure/High-Reliability Networks, Chair: Teruo Higashino  
Additonal PC members:  
Ana R. Cavalli (France) Tai-Yi Huang (Taiwan)  
Masakatsu Nishigaki (Japan) Shoji Yuen (Japan)
2. HW/SW Coverification and Cosynthesis, Chair: Pao-Ann Hsiung  
Additonal PC members:  
Rong-Guey Chang (Taiwan) Tai-Yi Huang (Taiwan)  
Jung-Yi Kuo (Taiwan) Alan Liu (Taiwan)  
Win-Bin See (Taiwan)
3. Hardware Verification, Co-chairs: Chung-Yang Huang, Bow-Yaw Wang  
Additonal PC members:  
Tai-Yi Huang (Taiwan) Masakatsu Nishigaki (Japan)

## Reviewers

Madhukar Anand	Constantinos Bartzis	Jing Chen
Ting-Shuo Chou	Edward T.H. Chu	Zhe Dang
Arvind Easwaran	Xiang Fu	Dimitra Giannakopoulou
Kiyoharu Hamaguchi	Ping Hao	Hiromi Hiraishi
Geng-Dian Huang	Kuang-Li Huang	Ranjit Jhala
Li Jiao	Jesung Kim	Moonzoo Kim
Masaaki Kondo	Rom Langerak	Dongdai Lin
Xinxin Liu	Zhiming Liu	Stephane Maag
Franco Mazzanti	Chris Myers	Kozo Okano
Hong Pan	Usa Sammapun	Oleg Sokolsky
Jin Sun	Kenji Taguchi	Yu-Che Tsai
Tatsuhiro Tsuchiya	Razvan Voicu	Liqiang Wang
Rui Xue	Ping Yang	Tuba Yavuz-Kahveci
Karen Yorav	Fang Yu	Jian Zhang

## Sponsoring Institutions

National Science Council, Taiwan, ROC  
Ministry of Education, Taiwan, ROC  
Institute of Information Science, Academia Sinica, Taiwan, ROC  
National Taiwan University (NTU), Taiwan, ROC  
Center for Information and Electronics Technologies (CIET), NTU, Taiwan, ROC  
SOC Center, NTU, Taiwan, ROC  
Graduate Institute of Electronic Engineering, NTU, Taiwan, ROC  
Synopsys, Inc.

# Table of Contents

## Keynote Speech

Games for Formal Design and Verification of Reactive Systems . . . . .	1
<i>Rajeev Alur</i>	
Evolution of Model Checking into the EDA Industry . . . . .	2
<i>Robert P. Kurshan</i>	
Abstraction Refinement . . . . .	7
<i>Pei-Hsin Ho</i>	

## Invited Speech

Tools for Automated Verification of Web Services . . . . .	8
<i>Tevfik Bultan, Xiang Fu, Jianwen Su</i>	
Theorem Proving Languages for Verification . . . . .	11
<i>Jean-Pierre Jouannaud</i>	
An Automated Rigorous Review Method for Verifying and Validating Formal Specifications . . . . .	15
<i>Shaoying Liu</i>	

## Papers

Toward Unbounded Model Checking for Region Automata . . . . .	20
<i>Fang Yu, Bow-Yaw Wang</i>	
Search Space Partition and Case Basis Exploration for Reducing Model Checking Complexity . . . . .	34
<i>Bai Su, Wenhui Zhang</i>	
Synthesising Attacks on Cryptographic Protocols . . . . .	49
<i>David Sinclair, David Gray, Geoff Hamilton</i>	
Büchi Complementation Made Tighter . . . . .	64
<i>Ehud Friedgut, Orna Kupferman, Moshe Y. Vardi</i>	
SAT-Based Verification of Safe Petri Nets . . . . .	79
<i>Shougo Ogata, Tatsuhiro Tsuchiya, Tohru Kikuno</i>	
Disjunctive Invariants for Numerical Systems . . . . .	93
<i>Jérôme Leroux</i>	

Validity Checking for Quantifier-Free First-Order Logic with Equality Using Substitution of Boolean Formulas . . . . .	108
<i>Atsushi Moritomo, Kiyoharu Hamaguchi, Toshinobu Kashiwabara</i>	
Fair Testing Revisited: A Process-Algebraic Characterisation of Conflicts . . . . .	120
<i>Robi Malik, David Streader, Steve Reeves</i>	
Exploiting Symmetries for Testing Equivalence in the Spi Calculus . . . . .	135
<i>Ivan Cibrario B., Luca Durante, Riccardo Sisto, Adriano Valenzano</i>	
Using Block-Local Atomicity to Detect Stale-Value Concurrency Errors . . . . .	150
<i>Cyrille Artho, Klaus Havelund, Armin Biere</i>	
Abstraction-Based Model Checking Using Heuristical Refinement . . . . .	165
<i>Kairong Qian, Albert Nymeyer</i>	
A Global Timed Bisimulation Preserving Abstraction for Parametric Time-Interval Automata . . . . .	179
<i>Tadaaki Tanimoto, Suguru Sasaki, Akio Nakata, Teruo Higashino</i>	
Design and Evaluation of a Symbolic and Abstraction-Based Model Checker . . . . .	196
<i>Serge Haddad, Jean-Michel Ili�, Kais Klai</i>	
Component-Wise Instruction-Cache Behavior Prediction . . . . .	211
<i>Abdur Rakib, Oleg Parshin, Stephan Thesing, Reinhard Wilhelm</i>	
Validating the Translation of an Industrial Optimizing Compiler . . . . .	230
<i>I. Gordin, R. Leviathan, A. Pnueli</i>	
Composition of Accelerations to Verify Infinite Heterogeneous Systems . . . . .	248
<i>S�bastien Bardin, Alain Finkel</i>	
Hybrid System Verification Is Not a Sinecure (The Electronic Throttle Control Case Study) . . . . .	263
<i>Ansgar Fehnker, Bruce H. Krogh</i>	
Providing Automated Verification in HOL Using MDGs . . . . .	278
<i>Tarek Mhamdi, Sof��ne Tahar</i>	
Specification, Abduction, and Proof . . . . .	294
<i>Konstantine Arkoudas</i>	
Introducing Structural Dynamic Changes in Petri Nets: Marked-Controlled Reconfigurable Nets . . . . .	310
<i>Marisa Llorens, Javier Oliver</i>	



Typeness for $\omega$ -Regular Automata .....	324
<i>Orna Kupferman, Gila Morgenstern, Aniello Murano</i>	
Partial Order Reduction for Detecting Safety and Timing Failures of Timed Circuits .....	339
<i>Denduang Pradubsuwun, Tomohiro Yoneda, Chris Myers</i>	
Mutation Coverage Estimation for Model Checking.....	354
<i>Te-Chang Lee, Pao-Ann Hsiung</i>	
Modular Model Checking of Software Specifications with Simultaneous Environment Generation .....	369
<i>Claudio de la Riva, Javier Tuya</i>	
Rabin Tree and Its Application to Group Key Distribution .....	384
<i>Hiroaki Kikuchi</i>	
Using Overlay Networks to Improve VoIP Reliability .....	392
<i>M. Karol, P. Krishnan, J.J. Li</i>	
Integrity-Enhanced Verification Scheme for Software-Intensive Organizations .....	402
<i>Wen-Kui Chang, Chun-Yuan Chen</i>	
RCGES: Retargetable Code Generation for Embedded Systems .....	415
<i>Trong-Yen Lee, Yang-Hsin Fan, Tsung-Hsun Yang, Chia-Chun Tsai, Wen-Ta Lee, Yuh-Shyan Hwang</i>	
Verification of Analog and Mixed-Signal Circuits Using Timed Hybrid Petri Nets .....	426
<i>Scott Little, David Walter, Nicholas Seegmiller, Chris Myers, Tomohiro Yoneda</i>	
First-Order LTL Model Checking Using MDGs .....	441
<i>Fang Wang, Sofiène Tahar, Otmane Ait Mohamed</i>	
Localizing Errors in Counterexample with Iteratively Witness Searching .....	456
<i>ShengYu Shen, Ying Qin, SiKun Li</i>	
Verification of WCDMA Protocols and Implementation .....	470
<i>Anyi Chen, Jian-Ming Wang, Chiu-Han Hsiao</i>	
Efficient Representation of Algebraic Expressions .....	474
<i>Tsung Lee, Pen-Ho Yu</i>	
Development of RTOS for PLC Using Formal Methods .....	479
<i>Jin Hyun Kim, Su-Young Lee, Young Ah Ahn, Jae Hwan Sim, Jin Seok Yang, Na Young Lee, Jin Young Choi</i>	

Reducing Parametric Automata:  
A Multimedia Protocol Service Case Study ..... 483  
*Lin Liu, Jonathan Billington*

Synthesis of State Feedback Controllers  
for Parameterized Discrete Event Systems ..... 487  
*Hans Bherer, Jules Desharnais, Marc Frappier, Richard St-Denis*

Solving Box-Pushing Games via Model Checking  
with Optimizations ..... 491  
*Gihwon Kwon, Taehoon Lee*

CLP Based Static Property Checking ..... 495  
*Tun Li, Yang Guo, SiKun Li*

A Temporal Assertion Extension to Verilog ..... 499  
*Kai-Hui Chang, Wei-Ting Tu, Yi-Jong Yeh, Sy-Yen Kuo*

**Author Index** ..... 505