

Thomas Ball
Robert B. Jones (Eds.)

LNCS 4144

Computer Aided Verification

18th International Conference, CAV 2006
Seattle, WA, USA, August 2006
Proceedings



Springer

TP311-53
C376
2006
Thomas Ball Robert B. Jones (Eds.)

Computer Aided Verification

18th International Conference, CAV 2006
Seattle, WA, USA, August 17-20, 2006
Proceedings



Springer



E200604019

Volume Editors

Thomas Ball
Microsoft Research
One Microsoft Way, Redmond, WA 98052, USA
E-mail: tball@microsoft.com

Robert B. Jones
Intel Corporation, RA2-459
2501 NW 229th Avenue, Hillsboro, OR 97124, USA
E-mail: robert.b.jones@acm.org

Library of Congress Control Number: 2006930415

CR Subject Classification (1998): F.3, D.2.4, D.2.2, F.4.1, I.2.3, B.7.2, C.3

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

ISSN	0302-9743
ISBN-10	3-540-37406-X Springer Berlin Heidelberg New York
ISBN-13	978-3-540-37406-0 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: 11817963 06/3142 5 4 3 2 1 0

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

Preface

This volume contains the proceedings of the International Conference on Computer Aided Verification (CAV), held in Seattle, Washington, USA, July 16–20, 2006. CAV 2006 was the 18th in a series of conferences dedicated to the advancement of the theory and practice of computer-assisted formal analysis methods for software and hardware systems. The conference covers the spectrum from theoretical results to concrete applications, with an emphasis on practical verification tools and the algorithms and techniques that are needed for their implementation.

We received 121 regular paper submissions and 23 tool paper submissions. Of these, the Program Committee selected 35 regular papers and 10 tool papers. Each submission was reviewed by three members of the Program Committee. In addition, each regular paper was reviewed by at least one expert external to the Program Committee.

The CAV 2006 program included five invited talks:

- Manuvir Das (Microsoft) on “Formal Specifications on Industrial-Strength Code—From Myth to Reality”
- David Dill (Stanford University) on “I Think I Voted: E-voting vs. Democracy”
- David Harel (Weizmann Institute) on “Playing with Verification, Planning and Aspects: Unusual Methods for Running Scenario-Based Programs”
- Tony Hoare (Microsoft) on “The Ideal of Verified Software”
- Joe Stoy (Bluespec) on “Verification? Getting it Right the First Time”

The traditional CAV tutorial was replaced by a special symposium, “25 Years of Model Checking,” organized by Orna Grumberg (Technion) and Helmut Veith (Technical University of Munich). The symposium consisted of 12 invited lectures delivered by leading researchers in the field of model checking.

This year, CAV was part of the Federated Logic Conference (FLoC 2006), and was jointly organized with ICLP (International Conference on Logic Programming), IJCAR (International Joint Conference on Automated Reasoning), LICS (Logic in Computer Science), RTA (Rewriting Techniques and Applications), and SAT (Theory and Applications of Satisfiability Testing). In particular, the invited talk by David Dill was a FLoC plenary talk, and the invited talk by David Harel was a FLoC keynote talk.

CAV 2006 had nine affiliated workshops:

- ACL2: 6th International Workshop on the ACL2 Theorem Prover and Its Applications (joint with IJCAR)
- BMC: 4th International Workshop on Bounded Model Checking
- CFV: Workshop on Constraints in Formal Verification
- FATES/FV: Formal Approaches to Testing and Runtime Verification (joint with IJCAR)

- GDV: Third Workshop on Games in Design and Verification
- SMT-COMP: Second Satisfiability Modulo Theories Competition
- TV: First Workshop on Multithreading in Hardware and Software: Formal Approaches to Design and Verification
- V&D: First International Workshop on Verification and Debugging
- VSTTE: Workshop on Verified Software: Theory, Tools, and Experiments

We gratefully acknowledge financial support for CAV 2006 from Cadence Design Systems, IBM, Intel Corporation, Microsoft Research, and NEC.

We thank the Program Committee members and the sub-referees for their work in evaluating the submissions. We appreciate the efforts of the Program Committee to attend the first physical PC meeting in the history of CAV. We thank Rance Cleveland and the University of Maryland for hosting the CAV PC meeting. We also thank the Steering Committee and the Chairs of CAV 2005 for their help and advice. Finally, we thank Andrei Voronkov for creating and supporting the outstanding EasyChair conference management system.

June 2006

Thomas Ball
Robert B. Jones

Conference Organization

Program Chairs

Thomas Ball (Microsoft Research, USA)
Robert B. Jones (Intel Corporation, USA)

Program Committee

Clark Barrett (New York University, USA)
Karthik Bhargavan (Microsoft Research, UK)
Per Bjesse (Synopsys, USA)
Ahmed Bouajjani (University of Paris 7, France)
Randy Bryant (Carnegie Mellon University, USA)
Rance Cleaveland (University of Maryland, USA)
Werner Damm (University of Oldenburg, Germany)
Steven German (IBM, USA)
Patrice Godefroid (Bell Labs, USA)
Ganesh Gopalakrishnan (University of Utah, USA)
Mike Gordon (University of Cambridge, UK)
Orna Grumberg (Technion, Israel)
Holger Hermanns (Saarland University, Germany)
Ranjit Jhala (University of California at San Diego, USA)
Roope Kaivola (Intel Corporation, USA)
Kenneth McMillan (Cadence Berkeley Labs, USA)
Tom Melham (Oxford University, UK)
Corina Pasareanu (NASA Ames, USA)
Amir Pnueli (New York University, USA)
Thomas Reps (University of Wisconsin, USA)
Sanjit Seshia (University of California at Berkeley, USA)
A. Prasad Sistla (University of Illinois at Chicago, USA)
Fabio Somenzi (University of Colorado, USA)

Steering Committee

Edmund M. Clarke (Carnegie Mellon University, USA)
Mike Gordon (University of Cambridge, UK)
Robert Kurshan (Cadence, USA)
Amir Pnueli (New York University, USA)

Corporate Sponsors

Cadence Design Systems
 IBM
 Intel Corporation
 Microsoft Research
 NEC

Referees

Fadi Aloul	Byron Cook	Ziyad Hanna
Flemming Anderson	Nathan Coopride	John Harrison
Gilad Arnold	Jordi Cortadella	Klaus Havelund
Tamarah Arons	Patrick Cousot	Keijo Heljanko
Eugene Asarin	Pedro R. D'Argenio	Martijn Hendriks
Ittai Balaban	Alexandre David	Marc Herbstritt
Gogul Balakrishnan	Dan Deavours	Pei-Hsin Ho
Thomas Ball	Saumya Debray	Michael Hsiao
Roberto Barbuti	Salem Derisavi	Hardi Hungar
Sharon Barner	Jyotirmoy Deshmukh	Michael Huth
Robert Bauer	Henning Dierks	Sonjong Hwang
Jason Baumgartner	Yaniv Eitani	Radu Iosif
Peter Beerel	Allen Emerson	Franjo Ivancic
Gerd Behrmann	Michael Ernst	Himanshu Jain
Josh Berdine	Javier Esparza	Somesh Jha
Eyal Bin	Cormac Flanagan	Sven Johr
Jesse Bingham	Martin Fränzle	Rajeev Joshi
Roderick Bloem	Zhaohui Fu	Comon Jurski
Bernard Boigelot	Vinod Ganapathy	Vineet Kahlon
Dragan Bosnacki	Paul Gastin	Shmuel Katz
John Mark Boulter	Biniam Gebremichael	Zurab Khasidashvili
Patricia Boyer	Rajnish Ghughal	Nick Kidd
Aaron R. Bradley	Dimitra Giannakopoulou	Hyondeuk Kim
Guillaume Brat	Amit Goel	Mike Kishinevsky
Laura Brandan Briones	Dieter Gollmann	Christoph Koch
Glenn Bruns	Denis Gopan	Alfred Koelbl
Tevfik Bultan	Alexey Gotsman	Sava Krstic
Sebastian Burckhardt	Susanne Graf	Hillel Kugler
Doron Bustan	Radu Grosu	Jim Kukula
Luca Carloni	Jim Grundy	Viktor Kuncak
Arindam Chakrabarti	Sumit Gulwani	Orna Kupferman
Feng Chen	Arie Gurfinkel	Shuvendu K. Lahiri
Xiaofang Chen	Aarti Gupta	Akash Lal
Hana Chockler	Peter Habermehl	Robby Lampert
Alessandro Cimatti	Hyojung Han	Rom Langerak

Marc Lettrari	John O’Leary	Deian Tabakov
Tel Lev-Ami	Robert Palmer	Murali Talulpur
Bing Li	Seungjoon Park	Ashish Tiwari
Junghee Lim	Paul Pettersson	Mark Tuttle
Alexey Loginov	Andreas Podelski	Rachel Tzoref
Michael Lowry	Lee Pike	Yaroslav S. Usenko
Tony Ma	Nir Piterman	Noppanunt Utamaphethai
P. Madhusudan	Shaz Qadeer	Moshe Vardi
Rupak Majumdar	Sriram K. Rajamani	Margus Veanes
Oded Maler	Kavita Ravi	Willem Visser
Roman Manevich	John Regehr	Tomas Vojnar
Freddy Mang	Jakob Rehof	Silke Wagner
Pete Manolios	Grigore Rosu	Igor Walukiewicz
Shahar Maoz	Andrey Rybalchenko	Dong Wang
Scott McPeak	Sriram Sankaranarayanan	Westley Weimer
Todd Millstein	Jun Sawada	Gera Weiss
Antoine Mine	Sven Schewe	Bernd Westphal
Hari Mony	Wolfram Schulte	Yichen Xie
In-Ho Moon	Koushik Sen	Avi Yadgar
John Moondanos	Traian Florin Serbanuta	Eran Yahav
Anca Muscholl	Olivier Serre	Yu Yang
Madan Musuvathi	Ilya Shlyakhter	Jin Yang
Chris Myers	Sharon Shoham	Wang Yi
Anders Møller	Mihaela Sighireanu	Greta Yorsh
Indira Nair	Eli Singerman	Aleksandr Zaks
Kedar Namjoshi	Marielle Stoelinga	Anna Zaks
Naren Narasimhan	Scott D. Stoller	
Dejan Nickovic	Ofer Strichman	

Lecture Notes in Computer Science

For information about Vols. 1–4014

please contact your bookseller or Springer

- Vol. 4144: T. Ball, R.B. Jones (Eds.), *Computer Aided Verification*. XV, 564 pages. 2006.
- Vol. 4127: E. Damiani, P. Liu (Eds.), *Data and Applications Security XX*. X, 319 pages. 2006.
- Vol. 4121: A. Biere, C.P. Gomes (Eds.), *Theory and Applications of Satisfiability Testing - SAT 2006*. XII, 438 pages. 2006.
- Vol. 4115: D.-S. Huang, K. Li, G.W. Irwin (Eds.), *Computational Intelligence and Bioinformatics, Part III*. XXI, 803 pages. 2006. (Sublibrary LNBI).
- Vol. 4114: D.-S. Huang, K. Li, G.W. Irwin (Eds.), *Computational Intelligence, Part II*. XXVII, 1337 pages. 2006. (Sublibrary LNAI).
- Vol. 4113: D.-S. Huang, K. Li, G.W. Irwin (Eds.), *Intelligent Computing, Part I*. XXVII, 1331 pages. 2006.
- Vol. 4112: D.Z. Chen, D. T. Lee (Eds.), *Computing and Combinatorics*. XIV, 528 pages. 2006.
- Vol. 4111: F.S. de Boer, M.M. Bonsangue, S. Graf, W.-P. de Roever (Eds.), *Formal Methods for Components and Objects*. VIII, 447 pages. 2006.
- Vol. 4108: J.M. Borwein, W.M. Farmer (Eds.), *Mathematical Knowledge Management*. VIII, 295 pages. 2006. (Sublibrary LNAI).
- Vol. 4106: T.R. Roth-Berghofer, M.H. Göker, H. A. Güvenir (Eds.), *Advances in Case-Based Reasoning*. XIV, 566 pages. 2006. (Sublibrary LNAI).
- Vol. 4104: T. Kunz, S.S. Ravi (Eds.), *Ad-Hoc, Mobile, and Wireless Networks*. XII, 474 pages. 2006.
- Vol. 4099: Q. Yang, G. Webb (Eds.), *PRICAI 2006: Trends in Artificial Intelligence*. XXVIII, 1263 pages. 2006. (Sublibrary LNAI).
- Vol. 4098: F. Pfenning (Ed.), *Term Rewriting and Applications*. XIII, 415 pages. 2006.
- Vol. 4097: X. Zhou, O. Sokolsky, L. Yan, E.-S. Jung, Z. Shao, Y. Mu, D.C. Lee, D. Kim, Y.-S. Jeong, C.-Z. Xu (Eds.), *Emerging Directions in Embedded and Ubiquitous Computing*. XXVII, 1034 pages. 2006.
- Vol. 4096: E. Sha, S.-K. Han, C.-Z. Xu, M.H. Kim, L.T. Yang, B. Xiao (Eds.), *Embedded and Ubiquitous Computing*. XXIV, 1170 pages. 2006.
- Vol. 4094: O. H. Ibarra, H.-C. Yen (Eds.), *Implementation and Application of Automata*. XIII, 291 pages. 2006.
- Vol. 4093: X. Li, O.R. Zaiane, Z. Li (Eds.), *Advanced Data Mining and Applications*. XXI, 1110 pages. 2006. (Sublibrary LNAI).
- Vol. 4092: J. Lang, F. Lin, J. Wang (Eds.), *Knowledge Science, Engineering and Management*. XV, 664 pages. 2006. (Sublibrary LNAI).
- Vol. 4090: S. Spaccapietra, K. Aberer, P. Cudré-Mauroux (Eds.), *Journal on Data Semantics VI*. XI, 211 pages. 2006.
- Vol. 4088: Z.-Z. Shi, R. Sadananda (Eds.), *Agent Computing and Multi-Agent Systems*. XVII, 827 pages. 2006. (Sublibrary LNAI).
- Vol. 4079: S. Etalle, M. Truszczyński (Eds.), *Logic Programming*. XIV, 474 pages. 2006.
- Vol. 4077: M.-S. Kim, K. Shimada (Eds.), *Advances in Geometric Modeling and Processing*. XVI, 696 pages. 2006.
- Vol. 4076: F. Hess, S. Pauli, M. Pohst (Eds.), *Algorithmic Number Theory*. X, 599 pages. 2006.
- Vol. 4075: U. Leser, F. Naumann, B. Eckman (Eds.), *Data Integration in the Life Sciences*. XI, 298 pages. 2006. (Sublibrary LNBI).
- Vol. 4074: M. Burmester, A. Yasinsac (Eds.), *Secure Mobile Ad-hoc Networks and Sensors*. X, 193 pages. 2006.
- Vol. 4073: A. Butz, B. Fisher, A. Krüger, P. Olivier (Eds.), *Smart Graphics*. XI, 263 pages. 2006.
- Vol. 4072: M. Harders, G. Székely (Eds.), *Biomedical Simulation*. XI, 216 pages. 2006.
- Vol. 4071: H. Sundaram, M. Naphade, J.R. Smith, Y. Rui (Eds.), *Image and Video Retrieval*. XII, 547 pages. 2006.
- Vol. 4070: C. Priami, X. Hu, Y. Pan, T.Y. Lin (Eds.), *Transactions on Computational Systems Biology V*. IX, 129 pages. 2006. (Sublibrary LNBI).
- Vol. 4069: F.J. Perales, R.B. Fisher (Eds.), *Articulated Motion and Deformable Objects*. XV, 526 pages. 2006.
- Vol. 4068: H. Schärfe, P. Hitzler, P. Øhrstrøm (Eds.), *Conceptual Structures: Inspiration and Application*. XI, 455 pages. 2006. (Sublibrary LNAI).
- Vol. 4067: D. Thomas (Ed.), *ECOOP 2006 – Object-Oriented Programming*. XIV, 527 pages. 2006.
- Vol. 4066: A. Rensink, J. Warmer (Eds.), *Model Driven Architecture – Foundations and Applications*. XII, 392 pages. 2006.
- Vol. 4065: P. Perner (Ed.), *Advances in Data Mining*. XI, 592 pages. 2006. (Sublibrary LNAI).
- Vol. 4064: R. Büschkes, P. Laskov (Eds.), *Detection of Intrusions and Malware & Vulnerability Assessment*. X, 195 pages. 2006.
- Vol. 4063: I. Gorton, G.T. Heineman, I. Crnkovic, H.W. Schmidt, J.A. Stafford, C.A. Szyperski, K. Wallnau (Eds.), *Component-Based Software Engineering*. XI, 394 pages. 2006.
- Vol. 4062: G. Wang, J.F. Peters, A. Skowron, Y. Yao (Eds.), *Rough Sets and Knowledge Technology*. XX, 810 pages. 2006. (Sublibrary LNAI).

- Vol. 4061: K. Miesenberger, J. Klaus, W. Zagler, A. Karshmer (Eds.), *Computers Helping People with Special Needs*. XXIX, 1356 pages. 2006.
- Vol. 4060: K. Futatsugi, J.-P. Jouannaud, J. Meseguer (Eds.), *Algebra, Meaning, and Computation*. XXXVIII, 643 pages. 2006.
- Vol. 4059: L. Arge, R. Freivalds (Eds.), *Algorithm Theory – SWAT 2006*. XII, 436 pages. 2006.
- Vol. 4058: L.M. Batten, R. Safavi-Naini (Eds.), *Information Security and Privacy*. XII, 446 pages. 2006.
- Vol. 4057: J.P.W. Pluim, B. Likar, F.A. Gerritsen (Eds.), *Biomedical Image Registration*. XII, 324 pages. 2006.
- Vol. 4056: P. Flocchini, L. Gasieniec (Eds.), *Structural Information and Communication Complexity*. X, 357 pages. 2006.
- Vol. 4055: J. Lee, J. Shim, S.-g. Lee, C. Bussler, S. Shim (Eds.), *Data Engineering Issues in E-Commerce and Services*. IX, 290 pages. 2006.
- Vol. 4054: A. Horváth, M. Telek (Eds.), *Formal Methods and Stochastic Models for Performance Evaluation*. VIII, 239 pages. 2006.
- Vol. 4053: M. Ikeda, K.D. Ashley, T.-W. Chan (Eds.), *Intelligent Tutoring Systems*. XXVI, 821 pages. 2006.
- Vol. 4052: M. Bugliesi, B. Preneel, V. Sassone, I. Wegener (Eds.), *Automata, Languages and Programming, Part II*. XXIV, 603 pages. 2006.
- Vol. 4051: M. Bugliesi, B. Preneel, V. Sassone, I. Wegener (Eds.), *Automata, Languages and Programming, Part I*. XXIII, 729 pages. 2006.
- Vol. 4049: S. Parsons, N. Maudet, P. Moraitis, I. Rahwan (Eds.), *Argumentation in Multi-Agent Systems*. XIV, 313 pages. 2006. (Sublibrary LNAI).
- Vol. 4048: L. Goble, J.-J.C. Meyer (Eds.), *Deontic Logic and Artificial Normative Systems*. X, 273 pages. 2006. (Sublibrary LNAI).
- Vol. 4047: M. Robshaw (Ed.), *Fast Software Encryption*. XI, 434 pages. 2006.
- Vol. 4046: S.M. Astley, M. Brady, C. Rose, R. Zwigelaar (Eds.), *Digital Mammography*. XVI, 654 pages. 2006.
- Vol. 4045: D. Barker-Plummer, R. Cox, N. Swoboda (Eds.), *Diagrammatic Representation and Inference*. XII, 301 pages. 2006. (Sublibrary LNAI).
- Vol. 4044: P. Abrahamsson, M. Marchesi, G. Succi (Eds.), *Extreme Programming and Agile Processes in Software Engineering*. XII, 230 pages. 2006.
- Vol. 4043: A.S. Atzeni, A. Liroy (Eds.), *Public Key Infrastructure*. XI, 261 pages. 2006.
- Vol. 4042: D. Bell, J. Hong (Eds.), *Flexible and Efficient Information Handling*. XVI, 296 pages. 2006.
- Vol. 4041: S.-W. Cheng, C.K. Poon (Eds.), *Algorithmic Aspects in Information and Management*. XI, 395 pages. 2006.
- Vol. 4040: R. Reulke, U. Eckardt, B. Flach, U. Knauer, K. Polthier (Eds.), *Combinatorial Image Analysis*. XII, 482 pages. 2006.
- Vol. 4039: M. Morisio (Ed.), *Reuse of Off-the-Shelf Components*. XIII, 444 pages. 2006.
- Vol. 4038: P. Ciancarini, H. Wiklicky (Eds.), *Coordination Models and Languages*. VIII, 299 pages. 2006.
- Vol. 4037: R. Gorrieri, H. Wehrheim (Eds.), *Formal Methods for Open Object-Based Distributed Systems*. XVII, 474 pages. 2006.
- Vol. 4036: O. H. Ibarra, Z. Dang (Eds.), *Developments in Language Theory*. XII, 456 pages. 2006.
- Vol. 4035: T. Nishita, Q. Peng, H.-P. Seidel (Eds.), *Advances in Computer Graphics*. XX, 771 pages. 2006.
- Vol. 4034: J. Münch, M. Vierimaa (Eds.), *Product-Focused Software Process Improvement*. XVII, 474 pages. 2006.
- Vol. 4033: B. Stiller, P. Reichl, B. Tuffin (Eds.), *Performativity Has its Price*. X, 103 pages. 2006.
- Vol. 4032: O. Etzion, T. Kuflik, A. Motro (Eds.), *Next Generation Information Technologies and Systems*. XIII, 365 pages. 2006.
- Vol. 4031: M. Ali, R. Dapoigny (Eds.), *Advances in Applied Artificial Intelligence*. XXIII, 1353 pages. 2006. (Sublibrary LNAI).
- Vol. 4029: L. Rutkowski, R. Tadeusiewicz, L.A. Zadeh, J.M. Zurada (Eds.), *Artificial Intelligence and Soft Computing – ICAISC 2006*. XXI, 1235 pages. 2006. (Sublibrary LNAI).
- Vol. 4028: J. Kohlas, B. Meyer, A. Schiper (Eds.), *Dependable Systems: Software, Computing, Networks*. XII, 295 pages. 2006.
- Vol. 4027: H.L. Larsen, G. Pasi, D. Ortiz-Arroyo, T. Andreasen, H. Christiansen (Eds.), *Flexible Query Answering Systems*. XVIII, 714 pages. 2006. (Sublibrary LNAI).
- Vol. 4026: P.B. Gibbons, T. Abdelzaher, J. Aspnes, R. Rao (Eds.), *Distributed Computing in Sensor Systems*. XIV, 566 pages. 2006.
- Vol. 4025: F. Eliassen, A. Montresor (Eds.), *Distributed Applications and Interoperable Systems*. XI, 355 pages. 2006.
- Vol. 4024: S. Donatelli, P.S. Thiagarajan (Eds.), *Petri Nets and Other Models of Concurrency – ICATPN 2006*. XI, 441 pages. 2006.
- Vol. 4021: E. André, L. Dybkjær, W. Minker, H. Neumann, M. Weber (Eds.), *Perception and Interactive Technologies*. XI, 217 pages. 2006. (Sublibrary LNAI).
- Vol. 4020: A. Bredenfeld, A. Jacoff, I. Noda, Y. Takahashi (Eds.), *RoboCup 2005: Robot Soccer World Cup IX*. XVII, 727 pages. 2006. (Sublibrary LNAI).
- Vol. 4019: M. Johnson, V. Vene (Eds.), *Algebraic Methodology and Software Technology*. XI, 389 pages. 2006.
- Vol. 4018: V. Wade, H. Ashman, B. Smyth (Eds.), *Adaptive Hypermedia and Adaptive Web-Based Systems*. XVI, 474 pages. 2006.
- Vol. 4017: S. Vassiliadis, S. Wong, T.D. Hämmäläinen (Eds.), *Embedded Computer Systems: Architectures, Modeling, and Simulation*. XV, 492 pages. 2006.
- Vol. 4016: J.X. Yu, M. Kitsuregawa, H.V. Leong (Eds.), *Advances in Web-Age Information Management*. XVII, 606 pages. 2006.

¥581.00元

Table of Contents

Invited Talks

Formal Specifications on Industrial-Strength Code—From Myth to Reality	1
<i>Manuvir Das</i>	
I Think I Voted: E-Voting vs. Democracy	2
<i>David Dill</i>	
Playing with Verification, Planning and Aspects: Unusual Methods for Running Scenario-Based Programs	3
<i>David Harel</i>	
The Ideal of Verified Software	5
<i>Tony Hoare</i>	

Session 1. Automata

Antichains: A New Algorithm for Checking Universality of Finite Automata	17
<i>Martin De Wulf, Laurent Doyen, Thomas A. Henzinger, Jean-Francois Raskin</i>	
Safrless Compositional Synthesis	31
<i>Orna Kupferman, Nir Piterman, Moshe Y. Vardi</i>	
Minimizing Generalized Büchi Automata	45
<i>Sudeep Juvekar, Nir Piterman</i>	

Session 2. Tools Papers

TICC: A Tool for Interface Compatibility and Composition	59
<i>B. Thomas Adler, Luca de Alfaro, Leandro Dias Da Silva, Marco Faella, Axel Legay, Vishwanath Raman, Pritam Roy</i>	
FAST Extended Release	63
<i>Sébastien Bardin, Jérôme Leroux, Gérald Point</i>	

Session 3. Arithmetic

Don't Care Words with an Application to the Automata-Based Approach for Real Addition	67
<i>Jochen Eisinger, Felix Klaedtke</i>	
A Fast Linear-Arithmetic Solver for DPLL(T)	81
<i>Bruno Dutertre, Leonardo de Moura</i>	

Session 4. SAT and Bounded Model Checking

Bounded Model Checking for Weak Alternating Büchi Automata	95
<i>Keijo Heljanko, Tommi Junttila, Misa Keinänen, Martin Lange, Timo Latvala</i>	
Deriving Small Unsatisfiable Cores with Dominators	109
<i>Roman Gershman, Maya Koifman, Ofer Strichman</i>	

Session 5. Abstraction/Refinement

Lazy Abstraction with Interpolants	123
<i>Kenneth L. McMillan</i>	
Using Statically Computed Invariants Inside the Predicate Abstraction and Refinement Loop	137
<i>Himanshu Jain, Franjo Ivančić, Aarti Gupta, Ilya Shlyakhter, Chao Wang</i>	
Counterexamples with Loops for Predicate Abstraction	152
<i>Daniel Kroening, Georg Weissenbacher</i>	

Session 6. Tools Papers

Cascade: C Assertion Checker and Deductive Engine	166
<i>Nikhil Sethi, Clark Barrett</i>	
YASM: A Software Model-Checker for Verification and Refutation	170
<i>Arie Gurfinkel, Ou Wei, Marsha Chechik</i>	

Session 7. Symbolic Trajectory Evaluation

SAT-Based Assistance in Abstraction Refinement for Symbolic Trajectory Evaluation	175
<i>Jan-Willem Roorda, Koen Claessen</i>	
Automatic Refinement and Vacuity Detection for Symbolic Trajectory Evaluation	190
<i>Rachel Tzoref, Orna Grumberg</i>	

Session 8. Property Specification and Verification

Some Complexity Results for System Verilog Assertions	205
<i>Doron Bustan, John Havlicek</i>	
Check It Out: On the Efficient Formal Verification of Live Sequence Charts	219
<i>Jochen Klose, Tobe Toben, Bernd Westphal, Hartmut Wittke</i>	

Session 9. Time

Symmetry Reduction for Probabilistic Model Checking	234
<i>Marta Kwiatkowska, Gethin Norman, David Parker</i>	
Communicating Timed Automata: The More Synchronous, the More Difficult to Verify	249
<i>Pavel Krčál, Wang Yi</i>	
Allen Linear (Interval) Temporal Logic – Translation to LTL and Monitor Synthesis	263
<i>Grigore Roşu, Saddek Bensalem</i>	

Session 10. Tools Papers

DIVINE – A Tool for Distributed Verification	278
<i>Jiří Barnat, Luboš Brim, Ivana Černá, Pavel Moravec, Petr Ročkal, Pavel Šimeček</i>	
EverLost: A Flexible Platform for Industrial-Strength Abstraction-Guided Simulation	282
<i>Flavio M. de Paula, Alan J. Hu</i>	

Session 11. Concurrency

Symbolic Model Checking of Concurrent Programs Using Partial Orders and On-the-Fly Transactions	286
<i>Vineet Kahlon, Aarti Gupta, Nishant Sinha</i>	
Model Checking Multithreaded Programs with Asynchronous Atomic Methods	300
<i>Koushik Sen, Mahesh Viswanathan</i>	
Causal Atomicity	315
<i>Azadeh Farzan, P. Madhusudan</i>	

Session 12. Trees, Pushdown Systems and Boolean Programs

Languages of Nested Trees	329
<i>Rajeev Alur, Swarat Chaudhuri, P. Madhusudan</i>	
Improving Pushdown System Model Checking	343
<i>Akash Lal, Thomas Reps</i>	
Repair of Boolean Programs with an Application to C	358
<i>Andreas Griesmayer, Roderick Bloem, Byron Cook</i>	

Session 13. Termination

Termination of Integer Linear Programs	372
<i>Mark Braverman</i>	
Automatic Termination Proofs for Programs with Shape-Shifting Heaps	386
<i>Josh Berdine, Byron Cook, Dino Distefano, Peter W. O'Hearn</i>	
Termination Analysis with Calling Context Graphs.....	401
<i>Panagiotis Manolios, Daron Vroon</i>	

Session 14. Tools Papers

TERMINATOR: Beyond Safety	415
<i>Byron Cook, Andreas Podelski, Andrey Rybalchenko</i>	
CUTE and jCUTE: Concolic Unit Testing and Explicit Path Model-Checking Tools	419
<i>Koushik Sen, Gul Agha</i>	

Session 15. Abstract Interpretation

SMT Techniques for Fast Predicate Abstraction.....	424
<i>Shuvendu K. Lahiri, Robert Nieuwenhuis, Albert Oliveras</i>	
The Power of Hybrid Acceleration.....	438
<i>Bernard Boigelot, Frédéric Herbreteau</i>	
Lookahead Widening	452
<i>Denis Gopan, Thomas Reps</i>	

Session 16. Tools Papers

The Heuristic Theorem Prover: Yet Another SMT Modulo Theorem Prover	467
<i>Kenneth Roe</i>	

LEVER: A Tool for Learning Based Verification	471
<i>Abhay Vardhan, Mahesh Viswanathan</i>	

Session 17. Memory Consistency

Formal Verification of a Lazy Concurrent List-Based Set Algorithm	475
<i>Robert Colvin, Lindsay Groves, Victor Luchangco, Mark Moir</i>	
Bounded Model Checking of Concurrent Data Types on Relaxed Memory Models: A Case Study	489
<i>Sebastian Burckhardt, Rajeev Alur, Milo M.K. Martin</i>	
Fast and Generalized Polynomial Time Memory Consistency Verification	503
<i>Amitabha Roy, Stephan Zeisset, Charles J. Fleckenstein, John C. Huang</i>	

Session 18. Shape Analysis

Programs with Lists Are Counter Automata	517
<i>Ahmed Bouajjani, Marius Bozga, Peter Habermehl, Radu Iosif, Pierre Moro, Tomáš Vojnar</i>	
Lazy Shape Analysis	532
<i>Dirk Beyer, Thomas A. Henzinger, Grégory Théoduloz</i>	
Abstraction for Shape Analysis with Fast and Precise Transformers	547
<i>Tal Lev-Ami, Neil Immerman, Mooly Sagiv</i>	
Author Index	563

Formal Specifications on Industrial-Strength Code—From Myth to Reality

(Invited Talk)

Manuvir Das

Center for Software Excellence
Microsoft Corporation
manuvir@microsoft.com

Abstract. The research community has long understood the value of formal specifications in building robust software. However, the adoption of any specifications beyond run-time assertions in industrial software has been limited. All of this has changed at Microsoft in the last few years. Today, formal specifications are a mandated part of the software development process in the largest Microsoft product groups. Millions of specifications have been added, and tens of thousands of bugs have been exposed and fixed in future versions of products under development. In addition, Windows public interfaces are formally specified and the Visual Studio compiler understands and enforces these specifications, meaning that programmers anywhere can now use formal specifications to make their software more robust.

How did this happen? The key ingredients of success were picking a critical programming error that costs software companies real money (buffer overruns), and building an incremental solution in which programmers obtain value proportional to their specification effort. The key technical aspects of this incremental approach include SAL, a lightweight specification language for describing memory access behaviour of C/C++ programs; espX, a heavyweight modular checker that enforces consistency between the code and the specification and validates memory accesses; and SALinfer, a lightweight global analysis that infers and inserts a large fraction of the memory specifications automatically.

The goal of this talk is to share the technical story of the insights that enabled SAL, espX and SALinfer, as well as the social and practical story of how we were able to move organizations with thousands of programmers to an environment where the use of specifications is routine.