

*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*

Antti Valmari (Ed.)

# Model Checking Software

13th International SPIN Workshop  
Vienna, Austria, March 30 – April 1, 2006  
Proceedings



Springer

## Volume Editor

Antti Valmari  
Tampere University of Technology  
Institute of Software Systems  
PO Box 553, 33101 Tampere, Finland  
E-mail: antti.valmari@tut.fi

Library of Congress Control Number: 2006922236

CR Subject Classification (1998): F.3, D.2.4, D.3.1, D.2

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

ISSN	0302-9743
ISBN-10	3-540-33102-6 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-33102-5 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](http://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: 11691617 06/3142 5 4 3 2 1 0

# Preface

The name “SPIN” refers both to a workshop on model checking and to a famous model checking tool. The SPIN workshop is an annual forum for practitioners and researchers interested in state space-based techniques for the validation and analysis of software and hardware systems, including communication protocols. It focuses on techniques based on explicit representations of state spaces, as implemented in the SPIN model checker or other tools, and techniques based on a combination of explicit representations with other representations. The SPIN model checker has proven to be particularly suited for the analysis of concurrent asynchronous systems. The workshop aims to encourage interaction and exchange of ideas with all related areas in software engineering. To promote interaction even further, many SPIN workshops have been held in conjunction with other meetings.

The 13th International SPIN Workshop on Model Checking of Software was held in Vienna, Austria, co-located with the European Joint Conferences on Theory and Practice of Software (ETAPS) 2006. The earlier SPIN workshops were held in Montreal, Canada (1995); Rutgers University, USA (1996); Twente University, The Netherlands (1997); ENST, Paris, France (1998); Trento, Italy (1999); Toulouse, France (1999); Stanford University, USA (2000); Toronto, Canada (2001); Grenoble, France (2002); Portland, Oregon, USA (2003); Barcelona, Spain (2004); and San Francisco, USA (2005). The proceedings of the Trento and Toulouse workshops were published together in Springer’s *Lecture Notes in Computer Science* volume 1680. From then on, each SPIN proceedings has been published as an individual LNCS volume.

SPIN 2006 attracted 44 submissions, of which 5 were short tool presentations and 7 were co-authored by a member of the Program Committee. The submissions were distributed to Program Committee members for reviewing. They reviewed the papers either personally or delegated them to sub-reviewers. The sub-reviewers are listed on page VIII. Each paper received three reviews, and in one case an additional fourth review was obtained.

Submissions whose reviews were neither overwhelmingly positive nor overwhelmingly negative were discussed by the Program Committee members. Most discussions led to a consensus on the fate of the paper. In the few cases where a disagreement remained to the end, the decision followed the opinion of the majority of the Program Committee members who had participated in the processing of that submission. All accepted papers had in the end more support (scores 4 and 5) than objection (scores 2, 1 and 0), and no rejected paper had more support than objection. Program committee members who had co-authored a submission, or for some other reason declared a conflict with it, were excluded from all information regarding its processing.

The Program Committee chose 19 submissions to be presented in the workshop and included in the proceedings. Of these, three were short tool presentations and four were co-authored by a member of the PC.

After processing the submitted papers, the Program Committee invited Roope Kaivola (Intel Corporation, USA) to give a keynote talk on the verification of microprocessors at Intel, and Stefan Edelkamp (Universität Dortmund, Germany) to give a tutorial on directed model checking.

The submission deadline of SPIN 2006 was set quite late, to position it reasonably relative to the submission deadlines of other conferences in the field. As a consequence, the Program Committee had to work in an unusually short period of time, perhaps the shortest in the recent history of SPIN. That the full number of reviews was obtained for each submission is a small miracle. I am grateful to every member of the Program Committee for their efficient and excellent work!

In addition to the Program Committee, the help of the SPIN Steering Committee, and in particular its chair, Pierre Wolper (Université de Liège, Belgium), was extremely important for the success of the paper selection process. On the practical side, the OCS Online Conference Service (originally developed by METAFrame) maintained by Martin Karusseit and Markus Bajohr at the University of Dortmund proved once again very helpful in various stages of the paper selection procedure. And, of course, without the hard work of local organizers there would not have been any workshop — our thanks to Jens Knoop, Andreas Krall, and their team.

January 2006

Antti Valmari  
Program Chair  
SPIN 2006

# Organization

SPIN 2006 was the 13th International SPIN Workshop on Model Checking of Software. It was held in Vienna, Austria, March 30–April 1, 2006. It was one of the satellite events of ETAPS 2006, The European Joint Conferences on Theory and Practice of Software. On behalf of ETAPS, Jens Knoop and Andreas Krall (Vienna University of Technology) took care of the practical organization of SPIN 2006 and other satellite events.

## Advisory Committee

Gerard Holzmann  
Amir Pnueli

## Steering Committee

Thomas Ball	Susanne Graf	Moshe Vardi
Patrice Godefroid	Stefan Leue	Pierre Wolper (Chair)

## Program Committee

Jonathan Billington (University of South Australia)  
Bernard Boigelot (University of Liège, Belgium)  
Dragan Bošnački (Eindhoven University of Technology, The Netherlands)  
Dennis Dams (Bell Labs, USA)  
Stefan Edelkamp (University of Dortmund, Germany)  
Cormac Flanagan (University of California at Santa Cruz, USA)  
Gerard Holzmann (NASA/JPL, USA)  
Roope Kaivola (Intel, USA)  
Lars M. Kristensen (University of Aarhus, Denmark)  
Stefan Leue (University of Konstanz, Germany)  
Laurent Mounier (Verimag, France)  
Wojciech Penczek (Polish Academy of Sciences, Poland)  
Bill Roscoe (University of Oxford, UK)  
Theo Ruys (University of Twente, The Netherlands)  
Stefan Schwoon (University of Stuttgart, Germany)  
Scott Stoller (SUNY at Stony Brook, USA)  
Antti Valmari (Tampere University of Technology, Finland) (Chair)  
Willem Visser (NASA Ames, USA)

## Additional Referees

Aljazzar, Husain	Groce, Alex	Orzechowski, Maciej
Andova, Suzana	Han, Bing	Paczkowski, Pawel
Bednarczyk, Marek	Hermanns, Holger	Ștefănescu, Alin
Bingham, Jesse	Ioustinova, Natalia	Stegantova, Evghenia
Borzyszkowski, Andrzej	Jabbar, Shahid	Szreter, Maciej
Bultan, Tevfik	Janowski, Pawel	Wei, Wei
Conway, Christopher	Joshi, Rajeev	Westergaard, Michael
Esser, Robert	Kellomäki, Timo	Wozna, Bozena
Gallasch, Guy Edward	Lluch Lafuente, Alberto	Yang, Ping
Ghughal, Rajnish	Namjoshi, Kedar	Zhang, Dezhuang
Goel, Amit	Narasimhan, Naren	
Graf, Susanne	Niewiadomski, Artur	

# Table of Contents

## Directed Model Checking

Large-Scale Directed Model Checking LTL <i>Stefan Edelkamp, Shahid Jabbar</i> .....	1
Directed Model Checking with Distance-Preserving Abstractions <i>Klaus Dräger, Bernd Finkbeiner, Andreas Podelski</i> .....	19
Adapting an AI Planning Heuristic for Directed Model Checking <i>Sebastian Kupferschmid, Jörg Hoffmann, Henning Dierks, Gerd Behrmann</i> .....	35
Larger Automata and Less Work for LTL Model Checking <i>Jaco Geldenhuys, Henri Hansen</i> .....	53

## Markovian Systems

<i>Don't Know</i> in Probabilistic Systems <i>Harald Fecher, Martin Leucker, Verena Wolf</i> .....	71
Symbolic Model Checking of Stochastic Systems: Theory and Implementation <i>Matthias Kuntz, Markus Siegle</i> .....	89

## Distributed Model Checking

Parallel and Distributed Model Checking in Eddy <i>Igor Melatti, Robert Palmer, Geoffrey Sawaya, Yu Yang, Robert Mike Kirby, Ganesh Gopalakrishnan</i> .....	108
Distributed On-the-Fly Model Checking and Test Case Generation <i>Christophe Joubert, Radu Mateescu</i> .....	126

## Advanced Handling of Data Aspects

Bounded Model Checking of Software Using SMT Solvers Instead of SAT Solvers <i>Alessandro Armando, Jacopo Mantovani, Lorenzo Platania</i> .....	146
Symbolic Execution with Abstract Subsumption Checking <i>Saswat Anand, Corina S. Păsăreanu, Willem Visser</i> .....	163



Abstract Matching for Software Model Checking <i>Pedro de la Cámara, María del Mar Gallardo, Pedro Merino</i> . . . . .	182
--	-----

## Applications

A Parametric State Space for the Analysis of the Infinite Class of Stop-and-Wait Protocols <i>Guy Edward Gallasch, Jonathan Billington</i> . . . . .	201
Verification of Medical Guidelines by Model Checking – A Case Study <i>Simon Bäumler, Michael Balser, Andriy Dunets, Wolfgang Reif, Jonathan Schmitt</i> . . . . .	219

## Assume–Guarantee

Towards a Compositional SPIN <i>Corina S. Păsăreanu, Dimitra Giannakopoulou</i> . . . . .	234
--	-----

## Partial Order Reduction

Exploiting Symmetry and Transactions for Partial Order Reduction of Rule Based Specifications <i>Ritwik Bhattacharya, Steven M. German, Ganesh Gopalakrishnan</i> . . . .	252
Partial-Order Reduction for General State Exploring Algorithms <i>Dragan Bošnački, Stefan Leue, Alberto Lluch Lafuente</i> . . . . .	271

## Tool Demonstrations

A Counterexample-Guided Refinement Tool for Open Procedural Programs <i>Aleksandar Dimovski, Dan R. Ghica, Ranko Lazić</i> . . . . .	288
jMosel: A Stand-Alone Tool and jABC Plugin for M2L(Str) <i>Christian Topnik, Eva Wilhelm, Tiziana Margaria, Bernhard Steffen</i> . . . . .	293
Model Checking Dynamic States in GROOVE <i>Harmen Kastenbergh, Arend Rensink</i> . . . . .	299
<b>Author Index</b> . . . . .	307