

Lecture Notes in Computer Science

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

1885

Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Klaus Havelund John Penix
Willem Visser (Eds.)

SPIN Model Checking and Software Verification

7th International SPIN Workshop
Stanford, CA, USA, August 30 – September 1, 2000
Proceedings

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Klaus Havelund
John Penix
Willem Visser
NASA Ames Research Center
Moffett Field, California 94035-1000, USA
E-mail: {havelund/jpenix/wvisser}@ptolemy.arc.nasa.gov

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

SPIN model checking and software verification : proceedings /
7th International SPIN Workshop, Stanford, CA, USA,
August 30 - September 1, 2000. Klaus Havelund ... (ed.) - Berlin ;
Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ;
Paris ; Singapore ; Tokyo : Springer, 2000
(Lecture notes in computer science ; Vol. 1885)
ISBN 3-540-41030-9

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

ISSN 0302-9743

ISBN 3-540-41030-9 Springer-Verlag 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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH
© Springer-Verlag Berlin Heidelberg 2000
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna
Printed on acid-free paper SPIN: 10722468 06/3142 5 4 3 2 1 0

Preface

The SPIN workshop is a forum for researchers interested in the subject of automata-based, explicit-state model checking technologies for the analysis and verification of asynchronous concurrent and distributed systems. The SPIN model checker (<http://netlib.bell-labs.com/netlib/spin/whatispin.html>), developed by Gerard Holzmann, is one of the best known systems of this kind, and has attracted a large user community. This can likely be attributed to its efficient state exploration algorithms. The fact that SPIN's modeling language, Promela, resembles a programming language has probably also contributed to its success.

Traditionally, the SPIN workshops present papers on extensions and uses of SPIN. As an experiment, this year's workshop was broadened to have a slightly wider focus than previous workshops in that papers on software verification were encouraged. Consequently, a small collection of papers describe attempts to analyze and verify programs written in conventional programming languages. Solutions include translations from source code to Promela, as well as specially designed model checkers that accept source code. We believe that this is an interesting research direction for the formal methods community, and that it will result in a new set of challenges and solutions. Of course, abstraction becomes the key solution to deal with very large state spaces. However, we also see potential for integrating model checking with techniques such as static program analysis and testing. Papers on these issues have therefore been included in the proceedings.

The workshop featured 17 refereed papers selected from 31 submissions, three invited talks, and three invited tutorials about commercial testing and formal methods tools, represented by three additional papers. Each refereed paper was reviewed by three reviewers. The three invited talks were as follows. Leslie Lamport (Compaq Systems Research Center) talked about model checking specifications; Bill Roscoe (Oxford University Computing Laboratory) talked about the FDR model checker and the verification of scalable real-life systems; and Peter Gluck (NASA's Jet Propulsion Laboratory) talked about testing of the Deep-Space 1 spacecraft software architecture. The three invited tutorials about commercial tools were as follows. Doron Drusinsky (Time Rover) presented the Temporal Rover tool, which performs temporal logic testing; Philippa Broadfoot and Bill Roscoe (Oxford University Computing Laboratory) presented the FDR model checker (developed by Formal Systems, of which Bill Roscoe was one of the founders); and Jerry Harrow (Compaq) presented the Visual Threads tool, which performs runtime analysis of multi-threaded programs.

The first SPIN workshop was held in October 1995 in Montréal. Subsequent workshops were held in New Brunswick (August 1996), Enschede (April 1997), Paris (November 1998), Trento (July 1999), and Toulouse (September 1999). This year's workshop ran for three days and was therefore the longest workshop to date.

Acknowledgments The editors of this volume wish to thank the program committee for its invaluable refereeing effort, resulting in a fine selection of papers. We also want to thank the additional referees supporting the program committee. Since each submitted paper received three reviews, the review effort was substantial. A special thanks goes to the Research Institute for Advanced Computer Science (RIACS) for sponsoring the event. We would also like to thank the Computational Sciences Division at the NASA Ames Research Center for generously providing resources.

August 2000

Klaus Havelund
John Penix
Willem Visser

Organization

SPIN 2000 was organized by the Automated Software Engineering Group within the Computational Sciences Division at the NASA Ames Research Center, California, USA.

Program Committee

Dennis Dams (Eindhoven University, The Netherlands)
David Dill (Stanford University, USA)
Orna Grumberg (The Technion, Israel)
John Hatcliff (Kansas State University, USA)
Bengt Jonsson (Uppsala University, Sweden)
Kim Larsen (Aalborg University, Denmark)
Stefan Leue (Albert-Ludwigs University, Germany)
Doron Peled (Bell Laboratories/Carnegie Mellon University, USA)
Natarajan Shankar (SRI International, USA)
Joseph Sifakis (Verimag, France)
Moshe Y. Vardi (Rice University, USA)
Pierre Wolper (Liege University, Belgium)

Organization

Klaus Havelund (QSS/Recom at NASA Ames Research Center, USA)
Gerard Holzmann (Bell Laboratories, USA)
John Penix (NASA Ames Research Center, USA)
Willem Visser (RIACS at NASA Ames Research Center, USA)

Referees

K. Altisen	M. Geilen	C. Păsăreanu
S. Bensalem	J. Geldenhuys	C. Pecheur
N. Bjørner	P. Godefroid	H. Saïdi
D. Bošnački	G. Goessler	N. Sidorova
M. Bozga	S. Graf	F. van Wijk
D. Bruening	F. Klaedtke	
P. Cuijpers	C. Muñoz	

Sponsoring Institution

Research Institute for Advanced Computer Science (RIACS), California, USA.

Table of Contents

Papers

Symmetric Spin.....	1
<i>Dragan Bošnački, Dennis Dams, and Leszek Holenderski</i> <i>(Eindhoven University of Technology)</i>	
Using Garbage Collection in Model Checking	20
<i>Radu Iosif and Riccardo Sisto (Politecnico di Torino)</i>	
Model Checking Based on Simultaneous Reachability Analysis	34
<i>Bengi Karaçalı and Kuo-Chung Tai (North Carolina State University)</i>	
Testing SPIN's LTL Formula Conversion into Büchi Automata with Randomly Generated Input	54
<i>Heikki Tauriainen and Keijo Heljanko (Helsinki University of Technology)</i>	
Verification and Optimization of a PLC Control Schedule	73
<i>Ed Brinksma (University of Twente) and Angelika Mader</i> <i>(University of Nijmegen)</i>	
Modeling the ASCB-D Synchronization Algorithm with SPIN: A Case Study	93
<i>Nicholas Weininger and Darren Cofer (Honeywell Technology Center)</i>	
Bebop: A Symbolic Model Checker for Boolean Programs	113
<i>Thomas Ball and Sriram K. Rajamani (Microsoft Research)</i>	
Logic Verification of ANSI-C Code with SPIN	131
<i>Gerard J. Holzmann (Lucent Technologies)</i>	
Interaction Abstraction for Compositional Finite State Systems	148
<i>Wayne Liu (University of Waterloo)</i>	
Correctness by Construction: Towards Verification in Hierarchical System Development	163
<i>Mila Majster-Cederbaum and Frank Salger (University of Mannheim)</i>	
Linking <i>STeP</i> with SPIN	181
<i>Anca Browne, Henny Sipma, and Ting Zhang (Stanford University)</i>	
Abstraction of Communication Channels in Promela: A Case Study	187
<i>Elena Fersman and Bengt Jonsson (Uppsala University)</i>	

A Language Framework for Expressing Checkable Properties of Dynamic Software 205
James C. Corbett (University of Hawaii), Matthew B. Dwyer, John Hatchiff, and Robby (Kansas State University)

Model-Checking Multi-threaded Distributed Java Programs 224
Scott D. Stoller (Indiana University)

Using Runtime Analysis to Guide Model Checking of Java Programs 245
Klaus Havelund (QSS/Recom at NASA Ames Research Center)

Communication Topology Analysis for Concurrent Programs 265
Mathieu Martel and Marc Gengler (Laboratoire d'Informatique de Marseille)

Low-Fat Recipes for SPIN 287
Theo C. Ruys (University of Twente)

Tool Tutorials

Tutorial on FDR and Its Applications 322
Philippa Broadfoot and Bill Roscoe (Oxford University)

The Temporal Rover and the ATG Rover 323
Doron Drusinsky (Time-Rover Inc.)

Runtime Checking of Multithreaded Applications with Visual Threads 331
Jerry J. Harrow (Compaq Computer Corporation)

Author Index 343