Lecture Notes in Computer Science 2318
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

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

Dragan Bošnački   Stefan Leue (Eds.)

Model Checking Software

9th International SPIN Workshop
Grenoble, France, April 11-13, 2002
Proceedings

Springer

Volume Editors

Dragan Bošnački
Eindhoven University of Technology
Faculty of Mathematics and Computer Science
P.O. Box 513, 5600 MB Eindhoven, The Netherlands
E-mail: dragan@win.tue.nl

Stefan Leue
Albert-Ludwigs-University Freiburg
Institute for Computer Science
Georges-Koehler-Allee Geb. 051, 79199 Freiburg, Germany
E-mail: leue@uni-freiburg.de

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Model checking software : proceedings / 9th International SPIN
Workshop, Grenoble, France, April 11 - 13, 2002. Dragan Bošnački ;
Stefan Leue (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ;
Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2318)
ISBN 3-540-43477-1

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

ISSN 0302-9743
ISBN 3-540-43477-1 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN 10846644 06/3142 5 4 3 2 1 0

Preface

The SPIN workshop series brings together researchers and practitioners interested in explicit state model checking technology as it is applied to the verification of software systems.

Since 1995, when the SPIN workshop series was instigated, SPIN workshops have been held on an annual basis at Montréal (1995), New Brunswick (1996), Enschede (1997), Paris (1998), Trento (1999), Toulouse (1999), Stanford (2000), and Toronto (2001). While the first SPIN workshop was a stand-alone event, later workshops have been organized as more or less closely affiliated events with larger conferences, in particular with CAV (1996), TACAS (1997), FORTE/PSTV (1998), FLOC (1999), World Congress on Formal Methods (1999), FMOODS (2000), and ICSE (2001). This year, SPIN 2002 was held as a satellite event of ETAPS 2002, the European Joint Conferences on Theory and Practice of Software. The co-location of SPIN workshops with conferences has proven to be very successful and has helped to disseminate SPIN model checking technology to wider audiences. Since 1999, the proceedings of the SPIN workshops have appeared in Springer-Verlag's "Lecture Notes in Computer Science" series.

The history of successful SPIN workshops is evidence for the maturing of model checking technology, not only in the hardware domain, but increasingly also in the software area. While in earlier years algorithms and tool development around the SPIN model checker[1] were the focus of this workshop series, the scope has recently widened to include more general approaches to software model checking. Current research in this area concentrates not so much on completely verifying system models, but rather on analyzing source code in order to discover software faults. The state space sizes that this analysis has to cope with require building adequate abstractions as well as algorithmic optimizations, which is reflected in a number of papers presented at SPIN 2002.

Out of the 20 research papers submitted, 10 were selected by the program committee. Every paper received three reviews. The reviewing and acceptance decision making for a submitted research paper for which one of the editors of this volume was a co-author was handled by a sub-committee chaired by Moshe Vardi. A further 3 out of the 20 submitted papers were accepted as extended abstracts in the "work in progress" category which was introduced to give emerging research ideas an opportunity for presentation. One submitted research paper was accepted as a tool demonstration. All three submitted tool presentations were accepted in that category. One tutorial was submitted, and it was also accepted in the tutorial category.

In addition to the selected technical program, SPIN 2002 featured two invited presentations. Edmund M. Clarke (Carnegie-Mellon University), one of the founding fathers of model checking technology, presented work on the use of SAT

[1] Freely available on the web from `http://netlib.bell-labs.com/netlib/spin/whatispin.html`.

solvers in the context of counterexample guided abstraction refinement. Patrick Cousot (ENS Paris), who pioneered research on abstract interpretation, talked about theory and practice of abstract interpretation. For the first time a SPIN workshop offered an invited beginners' tutorial aimed at teaching participants a) how to write models, and b) how to write models that can be efficiently analyzed by the SPIN model checker. This tutorial was given by Theo Ruys (University of Twente) and was open to all ETAPS 2002 participants.

Since overcoming barriers between academia and industry is essential to the advancement of model checking science and technology, industrial usage reports were invited for presentation, as in previous years, and included as extended abstracts into this proceedings volume. Cindy Eisner (IBM) and Doron Peled (University of Texas) presented a comparison of the use of symbolic and explicit model checking techniques in an industrial application environment. Per Bjesse (Prover Technology) discussed perspectives for and limitations of the industrial use of SAT-based model checking techniques. Finally, Yves-Marie Quemener (France Telecom) illustrated the use of model checking technology in the generation of test cases for XML-based telecommunications equipment.

Acknowledgements. The volume editors wish to thank all members of the program committee as well as the external reviewers for their tremendous effort which led to the selection of this year's program. We furthermore wish to thank ETAPS 2002 for inviting us to hold SPIN 2002 as a satellite event. Our particular appreciation goes to Susanne Graf, who acted as our liaison to ETAPS 2002, for accommodating the needs of SPIN 2002. Finally, we wish to thank METAFrame Technologies GmbH for allowing us to use their Conference Online Service system free of charge.

April 2002

Dragan Bošnački
Stefan Leue

Organization

SPIN 2002 was held in cooperation with ACM SIGPLAN as a satellite event of ETAPS 2002, the European Joint Conferences on Theory and Practice of Software, which was organized by the Laboratoire Verimag, Grenoble, France.

Organizing Committee

Program Chair: Stefan Leue (Albert-Ludwigs-University Freiburg, D)
Organizing Chair: Dragan Bošnački (Eindhoven University of Technology, NL)

Advisory Committee

Gerard Holzmann (Bell Labs, USA, chair)
Amir Pnueli (Weizmann, IL)

Steering Committee

Matt Dwyer (Kansas State, USA)
Stefan Leue (Freiburg, D)
Moshe Vardi (Rice, USA, chair)
Pierre Wolper (Liège, B)

Program Committee

Dragan Bošnački (Eindhoven, NL, organization chair)
Ed Brinksma (Twente, NL)
Marsha Chechik (Toronto, CA)
Dennis Dams (Bell Labs, USA and Eindhoven, NL)
Rob Gerth (Intel, USA)
Susanne Graf (Verimag, F)
John Hatcliff (Kansas State, USA)
Klaus Havelund (NASA Ames, USA)
Gerard Holzmann (Bell Labs, USA)
Bengt Jonsson (Uppsala, S)
Stefan Leue (Freiburg, D, chair)
Doron Peled (Austin, USA)
Sriram Rajamani (Microsoft Research, USA)
Riccardo Sisto (Torino, I)
Moshe Vardi (Rice, USA)
Willem Visser (NASA Ames, USA)
Pierre Wolper (Liège, B)

Referees

Victor Bos
Stefan Edelkamp
Leszek Holenderski
Angelika Mader
Corina Mitrohin
Theo Ruys

Table of Contents

Invited Talks

Invited Tutorial

Tutorial

Software Model Checking

Algorithms and Theoretical Foundations

Applications

Work in Progress

Invited Industrial Presentations

Model Checking Tools