Klaus Havelund, John Penix, Willem Visser (Eds.)

SPIN 2000

The 7th International SPIN Workshop
on Model Checking of Software.
Stanford University, California, USA.
August 30 - September 1, 2000.
Proceedings.

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, 3 invited talks, and 3 invited tutorials about commercial testing and formal methods tools, represented by 3 additional papers. Each refereed paper was reviewed by three reviewers. The 3 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 3 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 NASA Ames Research Center, California, USA.

Program Committee

Dennis Dams (Eindhoven University, Holland)
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/CMU, USA)
Natarajan Shankar (SRI, USA)
Joseph Sifakis (Verimag, France)
Moshe Y. Vardi (Rice University, USA)
Pierre Wolper (Université de Liege, 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
S. Bensalem
N. Bjørner
D. Bošnački
M. Bozga
D. Bruening
P. Cuijpers
M. Geilen
J. Geldenhuys
P. Godefroid
G. Goessler
S. Graf
F. Klaedtke
C. Muñoz
C. Păsăreanu
C. Pecheur
H. Saïdi
N. Sidorova
F. van Wijk

Sponsoring Institution

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

Table of Contents

Papers

Tool Tutorials