Lecture Notes in Computer Science 2989

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

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Susanne Graf   Laurent Mounier (Eds.)

Model Checking Software

11th International SPIN Workshop
Barcelona, Spain, April 1-3, 2004
Proceedings

Springer

Volume Editors

Susanne Graf
Laurent Mounier
VERIMAG
2, avenue de Vignate, 38610 Grenoble-Gières, France
E-mail: {Susanne.Graf, Laurent.Mounier}@imag.fr

Library of Congress Control Number: 2004102408

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

ISSN 0302-9743
ISBN 3-540-21314-7 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag is a part of Springer Science+Business Media

springeronline.com

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 10994757 06/3142 5 4 3 2 1 0

Preface

Since 1995, when the SPIN workshop series was instigated, SPIN workshops have been held on an annual basis in Montréal (1995), New Brunswick (1996), Enschede (1997), Paris (1998), Trento (1999), Toulouse (1999), Stanford (2000), Toronto (2001), Grenoble (2002) and Portland (2003). All but the first SPIN workshop were organized as satellite events of larger conferences, in particular of CAV (1996), TACAS (1997), FORTE/PSTV (1998), FLOC (1999), the World Congress on Formal Methods (1999), FMOODS (2000), ICSE (2001, 2003) and ETAPS (2002). This year again, SPIN was held as a satellite event of ETAPS 2004. 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 were the focus of this workshop series, for several years now the scope has been widened to include more general approaches to software model checking techniques and tools as well as applications.

The SPIN workshop has become a forum for all practitioners and researchers interested in model checking based techniques for the validation and analysis of communication protocols and software systems. Techniques based on explicit representations of state spaces, as implemented for example in the SPIN model checker or other tools, or techniques based on combinations of explicit representations with symbolic representations, are the focus of this workshop. It has proven to be particularly suitable for analyzing concurrent asynchronous systems. The workshop topics include theoretical and algorithmic foundations and tools, model derivation from code and code derivation from models, techniques for dealing with large and infinite state spaces, timing and applications. The workshop aims to encourage interactions and exchanges of ideas with all related areas in software engineering.

Papers went through a rigorous reviewing process. Each submitted paper was reviewed by three program committee members. Of 48 submissions, 19 research papers and 3 tool presentations were selected. Papers for which one of the editors was a co-author were handled by a sub-committee chaired by Gerard Holzmann.

In addition to the refereed papers, four invited talks were given; of these three were ETAPS invited speakers: Antti Valmari (Tampere, Finland) on the Rubik's Cube and what it can tell us about data structures, information theory and randomization, Mary-Lou Soffa (Pittsburgh, USA) on the foundations of code optimization, and Robin Milner (Cambridge, UK) on the grand challenge of building a theory for global ubiquitous computing. Finally, the SPIN invited speaker Reinhard Wilhelm (Saarbrücken, Germany) gave a talk on the analysis of timing models by means of abstract interpretation.

This year we took up an initiative started in 2002 and solicited tutorials that provided opportunities to get detailed insights into some validation tools and the methodologies of their use. Out of 3 submissions, the program committee selected 2 tutorials.

- An "advanced SPIN tutorial" giving an overview of recent extensions of the SPIN model checker as well as some methodological advice for its use. It was mainly addressed to users who want to use SPIN as a modelling and validation environment.
- A tutorial on the IF validation environment providing an overview of the IF modelling language and the main functionalities of the validation toolbox. It was addressed to users who want to use IF as a validation environment by feeding it with models in the IF language, or in SDL or UML, but also to tool developers who would like to interface their tools with the IF environment.

Acknowledgements. The volume editors wish to thank all members of the program committee as well as the external reviewers for their tremendous effort that led to the selection of this year's program. We furthermore wish to thank the organizers of ETAPS 2004 for inviting us to hold SPIN 2004 as a satellite event and for their support and flexibility in accommodating the particular needs of the SPIN workshop. We wish to thank in particular Fernando Orejas and Jordi Cortadella. Finally, we wish to thank Springer-Verlag for providing us with the possibility to use a conference online service free of charge, and the MetaFrame team, in particular Martin Karusseit, for their very valuable and reactive support.

January 2004

Susanne Graf
Laurent Mounier

Organization

SPIN 2004 was the 11th instance of the SPIN workshop on Model Checking of Software. It was held in cooperation with ACM SIGPLAN as a satellite event of ETAPS 2004, the European Joint Conferences on Theory and Practice of Software, which was organized by the Technical University of Catalonia in Barcelona, Spain.

Advisory Committee

Gerard Holzmann
Amir Pnueli

Steering Committee

Thomas Ball
Susanne Graf
Stefan Leue
Moshe Vardi
Pierre Wolper (chair)

Program Committee

Chairs: Susanne Graf (VERIMAG, Grenoble)
Laurent Mounier (VERIMAG, Grenoble)

Bernard Boigelot (Liège, Belgium)
Dragan Bošnački (Eindhoven, Netherlands)
David Dill (Stanford, USA)
Javier Esparza (Stuttgart, Germany)
Patrice Godefroid (Bell Labs, USA)
Susanne Graf (Grenoble, France)
John Hatcliff (Kansas State, USA)
Gerard Holzmann (NASA/JPL, USA)
Stefan Leue (Freiburg, Germany)
Pedro Merino (Malaga, Spain)
Laurent Mounier (Grenoble, France)
Mooly Sagiv (Tel Aviv, Israel)
Scott Stoller (Stony Brook, USA)
Antti Valmari (Tampere, Finland)

Reviewers

Robby
Suzana Andova
Gerd Behrmann
Saddek Bensalem
Marius Bozga
Cas Cremers
Maria del Mar Gallardo
Manuel Diaz
Jürgen Dingel
Jean-Claude Fernandez
Jaco Geldenhuys
Keijo Heljanko
Radu Iosif
Natalia Ioustinova
Rajeev Joshi
Tommi Junttila
Antero Kangas
Timo Karvi
Barbara König
Yassine Lakhnech
Johan Lilius
Jesus Martinez
Richard Mayr
Iulian Ober
Shaham Ohad
Michael Périn
Ilya Shlyakhter
Stavros Tripakis
Jaco van de Pol
Kimmo Varpaaniemi
Wei Wei
Tim Willemse
Eran Yahav
Ping Yang
Greta Yorsh

Table of Contents

Invited Paper

Formal Analysis of Processor Timing Models 1
Reinhard Wilhelm

Heuristics and Probabilities

Typical Structural Properties of State Spaces 5
Radek Pelánek

State Caching Reconsidered 23
Jaco Geldenhuys

Directed Error Detection in C++ with the Assembly-Level Model Checker StEAM 39
Peter Leven, Tilman Mehler, Stefan Edelkamp

Fast and Accurate Bitstate Verification for SPIN 57
Peter C. Dillinger, Panagiotis Manolios

Improvements of SPIN

Model-Driven Software Verification 76
Gerard J. Holzmann, Rajeev Joshi

Minimization of Counterexamples in SPIN 92
Paul Gastin, Pierre Moro, Marc Zeitoun

Validation of Timed Systems

Black-Box Conformance Testing for Real-Time Systems 109
Moez Krichen, Stavros Tripakis

Validation of UML Models via a Mapping to Communicating Extended Timed Automata 127
Iulian Ober, Susanne Graf, Ileana Ober

Tool Papers

Explicit State Model Checking with Hopper 146
Michael Jones, Eric Mercer

SEQ.OPEN: A Tool for Efficient Trace-Based Verification 151
Hubert Garavel, Radu Mateescu

Model Checking Genetic Regulatory Networks Using GNA and CADP .. 158
Grégory Batt, Damien Bergamini, Hidde de Jong, Hubert Garavel, Radu Mateescu

Abstraction and Symbolic Methods

Verification of Java Programs Using Symbolic Execution and Invariant Generation 164
Corina S. Păsăreanu, Willem Visser

Polynomial Time Image Computation with Interval-Definable Counters Systems 182
Alain Finkel, Jérôme Leroux

Using Fairness to Make Abstractions Work 198
Dragan Bošnački, Natalia Ioustinova, Natalia Sidorova

A Scalable Incomplete Test for Message Buffer Overflow in Promela Models 216
Stefan Leue, Richard Mayr, Wei Wei

Applications

Translation from Adapted UML to Promela for CORBA-Based Applications 234
J. Chen, H. Cui

Verifying Commit-Atomicity Using Model-Checking 252
Cormac Flanagan

Analysis of Distributed Spin Applied to Industrial-Scale Models 267
Murali Rangarajan, Samar Dajani-Brown, Kirk Schloegel, Darren Cofer

Verification of MPI-Based Software for Scientific Computation 286
Stephen F. Siegel, George S. Avrunin

Tutorials

Advanced SPIN Tutorial 304
Theo C. Ruys, Gerard J. Holzmann

IF Validation Environment Tutorial 306
Marius Bozga, Susanne Graf, Laurent Mounier, Iulian Ober

Author Index 309