

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

Alfred Kobsa

University of California, Irvine, CA, 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

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Ezio Bartocci C.R. Ramakrishnan (Eds.)

Model Checking Software

20th International Symposium, SPIN 2013
Stony Brook, NY, USA, July 8-9, 2013
Proceedings

Volume Editors

Ezio Bartocci
TU Wien
Faculty of Informatics
Favoritenstr. 9-11, 1084 Vienna, Austria
E-mail: ezio.bartocci@gmail.com

C.R. Ramakrishnan
Stony Brook University
Computer Science Department
Stony Brook, NY 11794-4400, USA
E-mail: cram@cs.stonybrook.edu

ISSN 0302-9743
ISBN 978-3-642-39175-0
DOI 10.1007/978-3-642-39176-7
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349
e-ISBN 978-3-642-39176-7

Library of Congress Control Number: 2013941132

CR Subject Classification (1998): D.2.4-5, D.2, D.3, F.3

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

© Springer-Verlag Berlin Heidelberg 2013

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the proceedings of the International SPIN Symposium on Model Checking of Software (SPIN 2013), which was held at Stony Brook University during July 8–9, 2013. SPIN 2013 marked the 20th anniversary of the SPIN workshop series.

The SPIN series is an annual forum for researchers and practitioners interested in verification of software systems. The traditional focus of SPIN has been on explicit-state model-checking techniques, as implemented in SPIN and other related tools. While such techniques are still of key interest to the workshop, its scope has broadened over recent years to include techniques for the verification and formal testing of software systems in general.

SPIN 2013 featured an invited lecture by Dirk Beyer (University of Passau) on “Reuse of Verification Results,” and an invited tutorial by Gerard Holzmann (NASA/JPL) on “Proving Properties of Concurrent Programs.” In his lecture, Dirk Beyer showed how the resources used in verification can be reduced by making the results of verification runs reusable. In particular, he focused on using conditional model checking, precision reuse, and verification witnesses to guide future verification runs. In his tutorial, Gerard Holzmann cited the increasing use of static analyzers in industrial software development, even though static analyzers yield false negatives as well as false positives. He then showed how SPIN can be used for analyzing multi-threaded programs, without false positives, while retaining some of the usability and speed of static analyzers.

SPIN 2013 received 40 submissions, from which the Program Committee accepted 18 regular papers and two tool demonstration papers. All papers received at least three reviews. The paper selection process involved extensive discussion among the members of the Program Committee and external reviewers. The status of the papers was decided once a consensus was reached in the committee.

We are extremely grateful to the members of the Program Committee and their sub-reviewers for their insightful reviews and discussion. The editors are also grateful to the authors of the accepted papers for revising the papers according to the suggestions of the Program Committee and for their responsiveness on providing the camera-ready copies within a tight deadline.

We would also like to thank Scott Smolka for serving as the General Chair, and the members of the SPIN Steering Committee and the Program Chairs of SPIN 2012, Alastair Donaldson and David Parker, for their advice on organizing and running the symposium. Special thanks go to Scott Stoller for his handling of all publicity-related matters while serving as the SPIN 2013 Publicity Chair. We thank Stony Brook University, and in particular, Ann Brody and Kathy Germana, for their valuable assistance with local organization. The EasyChair conference management system was used in the submission, review, and revision processes, as well as for the assembly of the symposium proceedings. We thank

the developers of EasyChair for this invaluable service. Finally, we thank IBM, Microsoft Research, NEC, and Nvidia for providing generous financial support to SPIN 2013.

May 2013

Ezio Bartocci
C.R. Ramakrishnan

Organization

Steering Committee

Dragan Bosnacki	Eindhoven University of Technology, The Netherlands
Susanne Graf	CNRS VERIMAG, France
Gerard Holzmann	NASA JPL, USA
Stefan Leue	University of Konstanz, Germany
Willem Visser	University of Stellenbosch, South Africa

General Chair

Scott A. Smolka	Stony Brook University, USA
-----------------	-----------------------------

Publicity Chair

Scott D. Stoller	Stony Brook University, USA
------------------	-----------------------------

Program Committee

Gogul Balakrishnan	NEC Labs, USA
Paolo Ballarini	Ecole Centrale Paris, France
Ezio Bartocci	TU Wien, Austria
Armin Biere	Johannes Kepler University, Austria
Marsha Chechik	University of Toronto, Canada
Hana Chockler	IBM, Israel
Giorgio Delzanno	Università di Genova, Italy
Alastair Donaldson	Imperial College London, UK
Dimitra Giannakopoulou	NASA Ames, USA
Patrice Godefroid	Microsoft Research, USA
Radu Grosu	TU Wien, Austria
Klaus Havelund	NASA JPL, USA
Gerard J. Holzman	NASA JPL, USA
Stefan Leue	University of Konstanz, Germany
Madanlal Musuvathi	Microsoft Research, USA
David Parker	University of Birmingham, UK
C.R. Ramakrishnan	Stony Brook University, USA
S. Ramesh	General Motors Global R&D, India
Stefan Schwoon	ENS Cachan, France
Scott A. Smolka	Stony Brook University, USA
Oleg Sokolsky	University of Pennsylvania, USA
Scott D. Stoller	Stony Brook University, USA
Stavros Tripakis	UC Berkeley, USA

VIII Organization

Helmut Veith
Farn Wang
Lenore Zuck

TU Wien, Austria
National Taiwan University, Taiwan
University of Illinois at Chicago, USA

Additional Reviewers

Aleksandrowicz, Gadi
Beer, Adrian
Bey, Alina
Bogomolov, Sergiy
Donzé, Alexandre
Elshuber, Martin
Gotsman, Alexey
Kahsai, Temesghen
Katsaros, Panagiotis
Ketema, Jeroen
Leitner-Fischer, Florian

Margalit, Oded
Rossetti, Daniele
Satpathy, Manoranjan
Seidl, Martina
Traverso, Riccardo
Von Essen, Christian
Wang, Shaohui
Wasicek, Armin
Widder, Josef
Yorav, Karen

Table of Contents

Reuse of Verification Results: Conditional Model Checking, Precision Reuse, and Verification Witnesses	1
<i>Dirk Beyer and Philipp Wendler</i>	
Proving Properties of Concurrent Programs (Extended Abstract)	18
<i>Gerard J. Holzmann</i>	
Verifying a Quantitative Relaxation of Linearizability via Refinement . . .	24
<i>Kiran Adhikari, James Street, Chao Wang, Yang Liu, and ShaoJie Zhang</i>	
A Map-Reduce Parallel Approach to Automatic Synthesis of Control Software	43
<i>Vadim Alimuguzhin, Federico Mari, Igor Melatti, Ivano Salvo, and Enrico Tronci</i>	
On-the-Fly Control Software Synthesis	61
<i>Vadim Alimuguzhin, Federico Mari, Igor Melatti, Ivano Salvo, and Enrico Tronci</i>	
Compositional Approach to Suspension and Other Improvements to LTL Translation	81
<i>Tomáš Babiak, Thomas Badie, Alexandre Duret-Lutz, Mojmír Krětinšký, and Jan Strejček</i>	
Regression Verification Using Impact Summaries	99
<i>John Backes, Suzette Person, Neha Rungta, and Oksana Tkachuk</i>	
Abstraction-Based Guided Search for Hybrid Systems	117
<i>Sergiy Bogomolov, Alexandre Donzé, Goran Frehse, Radu Grosu, Taylor T. Johnson, Hamed Ladan, Andreas Podelski, and Martin Wehrle</i>	
Probabilistic Verification of Coordinated Multi-robot Missions	135
<i>Sagar Chaki and Joseph Andrew Giampapa</i>	
Synthesizing Controllers for Automation Tasks with Performance Guarantees	154
<i>Chih-Hong Cheng, Michael Geisinger, and Christian Buckl</i>	
Specification and Validation of Link Reversal Routing via Graph Transformations	160
<i>Giorgio Delzanno and Riccardo Traverso</i>	

Local Model Checking of Weighted CTL with Upper-Bound Constraints	178
<i>Jonas Finnemann Jensen, Kim Guldstrand Larsen, Jiří Srba, and Lars Kaerlund Oestergaard</i>	
COMPL _e Te – A COMMunication Protocol vaLidation Toolchain	196
<i>Sven Gröning, Christopher Rosas, and Christian Wietfeld</i>	
Towards Modeling and Model Checking Fault-Tolerant Distributed Algorithms	209
<i>Annu John, Igor Konnov, Ulrich Schmid, Helmut Veith, and Josef Widder</i>	
Guard-Based Partial-Order Reduction	227
<i>Alfons Laarman, Elwin Pater, Jaco van de Pol, and Michael Weber</i>	
On the Synergy of Probabilistic Causality Computation and Causality Checking	246
<i>Florian Leitner-Fischer and Stefan Leue</i>	
Mining Sequential Patterns to Explain Concurrent Counterexamples	264
<i>Stefan Leue and Mitra Tabaei Befrouei</i>	
Automatic Equivalence Checking of UF+IA Programs	282
<i>Nuno P. Lopes and José Monteiro</i>	
Expression Reduction from Programs in a Symbolic Binary Executor	301
<i>Anthony Romano and Dawson Engler</i>	
Model Checking Unbounded Concurrent Lists	320
<i>Divyjit Sethi, Muralidhar Talupur, and Sharad Malik</i>	
Property-Driven Benchmark Generation	341
<i>Bernhard Steffen, Malte Isberner, Stefan Naujokat, Tiziana Margaria, and Maren Geske</i>	
Error-Completion in Interface Theories	358
<i>Stavros Tripakis, Christos Stergiou, Manfred Broy, and Edward A. Lee</i>	
Author Index	377