

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

Bernhard Beckert Ferruccio Damiani
Dilian Gurov (Eds.)

Formal Verification of Object-Oriented Software

International Conference, FoVeOOS 2011
Turin, Italy, October 5-7, 2011
Revised Selected Papers

Volume Editors

Bernhard Beckert
Karlsruhe Institute of Technology
Institute for Theoretical Informatics
Am Fasanengarten 5, 76131 Karlsruhe, Germany
E-mail: becker@kit.edu

Ferruccio Damiani
Università di Torino
Dipartimento di Informatica
Corso Svizzera 185, 10149 Torino
E-mail: ferruccio.damiani@unito.it

Dilian Gurov
KTH Royal Institute of Technology
School of Computer Science and Communications
Department of Theoretical Computer Science
100 44 Stockholm, Sweden
E-mail: dilian@csc.kth.se

ISSN 0302-9743
ISBN 978-3-642-31761-3
DOI 10.1007/978-3-642-31762-0
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349
e-ISBN 978-3-642-31762-0

Library of Congress Control Number: Applied for

CR Subject Classification (1998): D.2.3-4, D.2, D.1.3, D.1.5, D.3, F.3, K.6

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© Springer-Verlag Berlin Heidelberg 2012

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. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, 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.

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

Formal software verification has outgrown the area of academic case studies, and industry is showing serious interest. The logical next goal is the verification of industrial software products. Most programming languages used in industrial practice are object-oriented, e.g., Java, C++, or C#. The International Conference on Formal Verification of Object-Oriented Software (FoVeOOS 2011) aimed to foster collaboration and interactions among researchers in this area. It was held October 5–7, 2011, in Turin, Italy.

FoVeOOS was organized by COST Action IC0701 (www.cost-ic0701.org), but it went beyond the framework of this action. The conference was open to the whole scientific community. All submitted papers were peer-reviewed, and of the 28 submissions, the Program Committee selected 19 for presentation at the conference. In addition to the contributed papers, the program of FoVeOOS 2011 included four excellent keynote talks. We are grateful to Alan Mycroft (Cambridge University), James J. Hunt (aicas incorporated), Anindya Banerjee (IMDEA Software) and Peter Wong (Fredhopper) for accepting the invitation to address the conference.

This volume contains a selection of research papers and system descriptions presented at FoVeOOS 2011. The authors of all 19 papers presented at the conference were invited to submit improved versions, to be reviewed a second time. Of the 17 revised papers that were submitted, the Program Committee selected 10 for publication in this volume. Additionally, one of the invited speakers provided a one-page abstract, and the other three provided papers, which were all reviewed by the Program Committee. This volume also includes an invited paper reporting on the experiences with the program verification competition held during FoVeOOS 2011. This paper was also reviewed by the Program Committee.

We wish to sincerely thank all the authors who submitted their work for consideration. We also thank the Program Committee members as well as the additional referees for their great effort and professional work in the review and selection process. Their names are listed on the following pages.

It was a team effort that made the conference so successful. We particularly thank Sara Capecchi, Sarah Grebing, Vladimir Klebanov and Luca Padovani for their hard work and help in making the conference a success. In addition, we gratefully acknowledge the generous support of COST Action IC0701, the Karlsruhe Institute of Technology, the Museo Regionale di Scienze Naturali (MRSN) of Turin, and the University of Turin.

May 2012

Bernhard Beckert
Ferruccio Damiani
Dilian Gurov

Organization

Program Committee

Bernhard Beckert	Karlsruhe Institute of Technology, Germany
Frank S. de Boer	CWI, The Netherlands
Marcello Bonsangue	Universiteit Leiden (LIACS), The Netherlands
Einar Broch Johnsen	University of Oslo, Norway
Gabriel Ciobanu	ICS, Romanian Academy, Iași, Romania
Mads Dam	KTH Royal Institute of Technology, Stockholm, Sweden
Ferruccio Damiani	University of Turin, Italy
Sophia Drossopoulou	Imperial College, UK
Paola Giannini	University Piemonte Orientale, Italy
Dilian Gurov	KTH Royal Institute of Technology, Stockholm, Sweden
Reiner Hähnle	Chalmers University of Technology, Gothenburg, Sweden
Marieke Huisman	University of Twente, The Netherlands
Bart Jacobs	Katholieke Universiteit Leuven, Belgium
Thomas Jensen	INRIA Rennes, France
Ioannis Kassis	ETH Zürich, Switzerland
Joe Kiniry	ITU Copenhagen, Denmark
Vladimir Klebanov	Karlsruhe Institute of Technology, Germany
Dorel Lucanu	University Alexandru Ioan Cuza, Romania
María del Mar Gallardo	University of Málaga, Spain
Claude Marché	INRIA Saclay-Île-de-France, France
Julio Mariño	Universidad Politécnica de Madrid, Spain
Marius Minea	Politehnica University of Timișoara, Romania
Anders Møller	University Aarhus, Denmark
Rosemary Monahan	NUI Maynooth, Ireland
Wojciech Mostowski	Radboud University Nijmegen, The Netherlands
James Noble	Victoria University of Wellington, New Zealand
Bjarte M. Østvold	Norwegian Computing Center, Norway
Olaf Owe	University of Oslo, Norway
Matthew Parkinson	Cambridge University, UK
David Pichardie	IRISA, France
Frank Piessens	Katholieke Universiteit Leuven, Belgium
Ernesto Pimentel	University of Málaga, Spain
Arnd Poetzsch-Heffter	University of Kaiserslautern, Germany
Erik Poll	University of Nijmegen, The Netherlands

António Ravara	New University of Lisbon, Portugal
Wolfgang Reif	University of Augsburg, Germany
René Rydhof Hansen	University of Aalborg, Denmark
Ina Schaefer	Technical University of Braunschweig, Germany
Peter H. Schmitt	Karlsruhe Institute of Technology, Germany
Aleksy Schubert	University of Warsaw, Poland
Gheorghe Stefanescu	University of Bucharest, Romania
Bent Thomsen	University of Aalborg, Denmark
Shmuel Tyszberowicz	University of Tel Aviv, Israel
Tarmo Uustalu	Institute of Cybernetics, Tallinn, Estonia
Burkhard Wolff	University Paris-Sud (Orsay), France
Amiram Yehudai	University of Tel Aviv, Israel
Elena Zucca	University of Genova, Italy

Program Co-chairs

Ferruccio Damiani	University of Turin, Italy
Dilian Gurov	KTH Stockholm, Sweden

Organizing Committee

Bernhard Beckert	Karlsruhe Institute of Technology, Germany
Sara Capestri	University of Turin, Italy
Ferruccio Damiani	University of Turin, Italy
Dilian Gurov	KTH Stockholm, Sweden
Vladimir Klebanov	Karlsruhe Institute of Technology, Germany
Luca Padovani	University of Turin, Italy

Sponsoring Institutions

COST Action IC0701 “Formal Verification of Object-Oriented Software”
Karlsruhe Institute of Technology
Museo Regionale di Scienze Naturali (MRSN), Turin
University of Turin

Additional Referees

Richard Bubel	Axel Habermaier	Jurriaan Rot
Delphine Demange	Michiel Helvensteijn	Gerhard Schellhorn
Gidon Ernst	Ilham W. Kurnia	

Table of Contents

Invited Papers

Modular Verification of Object-Based Programs: Abstract of Invited Talk	1
<i>Anindya Banerjee</i>	
The COST IC0701 Verification Competition 2011	3
<i>Thorsten Bormer, Marc Brockschmidt, Dino Distefano, Gidon Ernst, Jean-Christophe Filliâtre, Radu Grigore, Marieke Huisman, Vladimir Klebanov, Claude Marché, Rosemary Monahan, Wojciech Mostowski, Nadia Polikarpova, Christoph Scheben, Gerhard Schellhorn, Bogdan Tofan, Julian Tschannen, and Mattias Ulbrich</i>	
The Practical Application of Formal Methods: Where Is the Benefit for Industry?	22
<i>James J. Hunt</i>	
Isolation Types and Multi-core Architectures	33
<i>Alan Mycroft</i>	
Modelling Adaptable Distributed Object Oriented Systems Using the HATS Approach: A Fredhopper Case Study	49
<i>Peter Y.H. Wong, Nikolay Diakov, and Ina Schaefer</i>	

Contributed Papers

Modeling and Analyzing the Interaction of C and C++ Strings	67
<i>Gogul Balakrishnan, Naoto Maeda, Sriram Sankaranarayanan, Franjo Ivančić, Aarti Gupta, and Rakesh Pothengil</i>	
Integration of Bounded Model Checking and Deductive Verification	86
<i>Bernhard Beckert, Thorsten Bormer, Florian Merz, and Carsten Sinz</i>	
A Probabilistic Framework for Object-Oriented Modeling and Analysis of Distributed Systems	105
<i>Lucian Bentea and Olaf Owe</i>	
Automated Detection of Non-termination and <code>NullPointerException</code> for Java Bytecode	123
<i>Marc Brockschmidt, Thomas Ströder, Carsten Otto, and Jürgen Giesl</i>	
<i>Juggernaut</i> – An Abstract JVM	142
<i>Jonathan Heinen, Henrik Barthels, and Christina Jansen</i>	

A Verified Implementation of Priority Monitors in Java	160
<i>Ángel Herranz and Julio Mariño</i>	
Scheduler-Specific Confidentiality for Multi-threaded Programs and Its Logic-Based Verification	178
<i>Marieke Huisman and Tri Minh Ngo</i>	
A Formal Model of User-Defined Resources in Resource-Restricted Deployment Scenarios	196
<i>Einar Broch Johnsen, Rudolf Schlatte, and S. Lizeth Tapia Tarifa</i>	
A \mathbb{K} -Based Formal Framework for Domain-Specific Modelling Languages	214
<i>Vlad Rusu and Dorel Lucanu</i>	
Verification of Information Flow Properties of JAVA Programs without Approximations	232
<i>Christoph Scheben and Peter H. Schmitt</i>	
Author Index	251