

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 Claude Marché (Eds.)

Formal Verification of Object-Oriented Software

International Conference, FoVeOOS 2010
Paris, France, June 28-30, 2010
Revised Selected Papers

Volume Editors

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

Claude Marché
INRIA Saclay – Île-de-France, Parc Orsay Université
4 rue Jacques Monod, 91893 Orsay Cedex, France
E-mail: Claude.Marche@inria.fr

Library of Congress Control Number: 2010941559

CR Subject Classification (1998): D.2.4, D.2, D.1.5, F.3, D.3, K.6, F.4

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN	0302-9743
ISBN-10	3-642-18069-8 Springer Berlin Heidelberg New York
ISBN-13	978-3-642-18069-9 Springer Berlin Heidelberg New York

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.

springer.com

© Springer-Verlag Berlin Heidelberg 2011
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

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 2010) aimed to foster collaboration and interaction among researchers in this area. It was held during June 28–30, 2010 in Paris, France.

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 35 submissions, the Program Committee selected 23 for presentation at the conference. In addition to the contributed papers, the program of FoVeOOS 2010 included three excellent keynote talks. We are grateful to June Andronick (NICTA, Sydney, Australia), Kim G. Larsen (Aalborg University, Denmark), Francesco Logozzo (Microsoft Research, Redmond, USA) for accepting the invitation to address the conference.

This volume contains a selection of research papers and system descriptions presented at FoVeOOS 2010. Authors of the 23 papers presented at the conference¹ were invited to submit improved versions, to be reviewed a second time. Twenty-one submissions were received, and the Program Committee selected 11 of them. Additionally, two of the invited speakers provided papers, which were reviewed by the Program Committee and included in this volume.

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 Sarah Grebing, Vladimir Klebanov, and Emmanuelle Perrot for their hard work and help in making the conference a success. In addition, we gratefully acknowledge the generous support of COST Action IC0701, Microsoft Research Redmond, the Institut National de Recherche en Informatique et Automatique (INRIA), and the Karlsruhe Institute of Technology

October 2010

Bernhard Beckert
Claude Marché

¹ Proceedings containing all papers presented at the conference are available at <http://digbib.ubka.uni-karlsruhe.de/volltexte/1000019083>.

Organization

Program Committee

Gilles Barthe	IMDEA Software, Madrid, Spain
Bernhard Beckert	Karlsruhe Institute of Technology, Germany
Einar Broch Johnsen	University of Oslo, Norway
Gabriel Ciobanu	University Alexandru Ioan Cuza, Romania
Dave Clarke	Katholieke University Leuven, Belgium
Mads Dam	KTH Stockholm, Sweden
Ferruccio Damiani	University of Turin, Italy
Sophia Drossopoulou	Imperial College, UK
Paola Giannini	University Piemonte Orientale, Italy
Dilian Gurov	KTH Stockholm, Sweden
Reiner Hähnle	Chalmers University of Technology, Gothenburg, Sweden
Marieke Huisman	University of Twente, The Netherlands
Thomas Jensen	IRISA/CNRS, France
Joe Kiniry	ITU Copenhagen, Denmark
Viktor Kuncak	EPF Lausanne, Switzerland
Dorel Lucanu	University Alexandru Ioan Cuza, Romania
María del Mar Gallardo	University of Malaga, Spain
Claude Marché	INRIA Saclay-Île-de-France, France
Julio Mariño	Universidad Politécnica de Madrid, Spain
Marius Minea	“Politehnica” University of Timisoara, Romania
Anders Møller	University of Aarhus, Denmark
Rosemary Monahan	NUI Maynooth, Ireland
Wojciech Mostowski	University of Nijmegen, The Netherlands
Peter Müller	ETH Zürich, Switzerland
James Noble	Victoria University of Wellington, New Zealand
Olaf Owe	University of Oslo, Norway
Ernesto Pimentel Sánchez	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

VIII Organization

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
Burkhardt Wolff	University Paris-Sud (Orsay), France
Elena Zucca	University of Genova, Italy

Program Co-chairs

Bernhard Beckert	Karlsruhe Institute of Technology, Germany
Claude Marché	INRIA Saclay-Île-de-France, France

Organizing Committee

Claude Marché (<i>Chair</i>)	INRIA Saclay-Île-de-France, France
Bernhard Beckert	Karlsruhe Institute of Technology, Germany
Vladimir Klebanov	Karlsruhe Institute of Technology, Germany
Emmanuelle Perrot	INRIA Saclay-Île-de-France, France

Sponsoring Institutions

COST Action IC0701 “Formal Verification of Object-Oriented Software”
Institut National de Recherche en Informatique et Automatique (INRIA)
Karlsruhe Institute of Technology
Microsoft Research

Additional Referees

Davide Ancona	Christoph Feller	Mads Chr. Olesen
Mohamed Faouzi Atig	Pietro Ferrara	Gerhard Schellhorn
Viviana Bono	Kathrin Geilmann	Martin Steffen
Daniel Bruns	Christoph Gladisch	Kurt Stenzel
Richard Bubel	Clément Hurlin	Volker Stolz
Jacek Chrzaszcz	Ioannis Kassios	Cristian Prisacariu
João Costa Seco	Ilham Kurnia	Bogdan Tofan
Delphine Demange	Laurent Mauborgne	Varmo Vene
Johan Dovland	Ruben Monjaraz	Amiram Yehudai
David Faitelson	Keiko Nakata	Greta Yorsh

Table of Contents

From a Proven Correct Microkernel to Trustworthy Large Systems	1
<i>June Andronick</i>	
Static Contract Checking with Abstract Interpretation	10
<i>Manuel Fähndrich and Francesco Logozzo</i>	
Abstract Compilation of Object-Oriented Languages into Coinductive CLP(X): Can Type Inference Meet Verification?	31
<i>Davide Ancona, Andrea Corradi, Giovanni Lagorio, and Ferruccio Damiani</i>	
Validating Timed Models of Deployment Components with Parametric Concurrency	46
<i>Einar Broch Johnsen, Olaf Owe, Rudolf Schlatte, and Silvia Lizeth Tapia Tarifa</i>	
Verification of Software Product Lines with Delta-Oriented Slicing	61
<i>Daniel Bruns, Vladimir Klebanov, and Ina Schaefer</i>	
Satisfiability Solving and Model Generation for Quantified First-Order Logic Formulas	76
<i>Christoph D. Gladisch</i>	
Sawja: Static Analysis Workshop for Java	92
<i>Laurent Hubert, Nicolas Barré, Frédéric Besson, Delphine Demange, Thomas Jensen, Vincent Monfort, David Pichardie, and Tiphaine Turpin</i>	
CVPP: A Tool Set for Compositional Verification of Control-Flow Safety Properties	107
<i>Marieke Huisman and Dilian Gurov</i>	
Specifying Imperative ML-Like Programs Using Dynamic Logic	122
<i>Séverine Maingaud, Vincent Balat, Richard Bubel, Reiner Hähnle, and Alexandre Miquel</i>	
Dynamic Frames in Java Dynamic Logic	138
<i>Peter H. Schmitt, Mattias Ulbrich, and Benjamin Weiß</i>	
A Refinement Methodology for Object-Oriented Programs	153
<i>Asma Tafat, Sylvain Boulmé, and Claude Marché</i>	

A Dynamic Logic for Unstructured Programs with Embedded Assertions.....	168
<i>Mattias Ulbrich</i>	
JMLUnit: The Next Generation.....	183
<i>Daniel M. Zimmerman and Rinkesh Nagmoti</i>	
Author Index	199