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 conference 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 Marín
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
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

Burkhart 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 *(Chair)*  
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
  June Andronick

Static Contract Checking with Abstract Interpretation.................... 10
  Manuel Fähndrich and Francesco Logozzo

Abstract Compilation of Object-Oriented Languages into Coinductive
CLP(X): Can Type Inference Meet Verification? ......................... 31
  Davide Ancona, Andrea Corradi, Giovanni Lagorio, and
  Ferruccio Damiani

Validating Timed Models of Deployment Components with Parametric
Concurrency ...................................................... 46
  Einar Broch Johnsen, Olaf Owe, Rudolf Schlatte, and
  Silvia Lizeth Tapia Tarifa

Verification of Software Product Lines with Delta-Oriented Slicing ...... 61
  Daniel Bruns, Vladimir Klebanov, and Ina Schaefer

Satisfiability Solving and Model Generation for Quantified First-Order
Logic Formulas ................................................. 76
  Christoph D. Gladisch

Sawja: Static Analysis Workshop for Java ............................ 92
  Laurent Hubert, Nicolas Barré, Frédéric Besson,
  Delphine Demange, Thomas Jensen, Vincent Monfort,
  David Pichardie, and Tiphaine Turpin

CVPP: A Tool Set for Compositional Verification of Control–Flow
Safety Properties .................................................. 107
  Marieke Huisman and Dilian Gurov

Specifying Imperative ML-Like Programs Using Dynamic Logic ...... 122
  Séverine Maingaud, Vincent Balat, Richard Bubel,
  Reiner Hähne, and Alexandre Miquel

Dynamic Frames in Java Dynamic Logic ................................ 138
  Peter H. Schmitt, Mattias Ulbrich, and Benjamin Weiß

A Refinement Methodology for Object-Oriented Programs ............. 153
  Asma Tafat, Sylvain Boulmé, and Claude Marché
A Dynamic Logic for Unstructured Programs with Embedded Assertions .......................... 168

Mattias Ulbrich

JMLUnit: The Next Generation .................................................. 183

Daniel M. Zimmerman and Rinkesh Nagmoti

Author Index .......................... 199