

*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*

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

*University of Dortmund, Germany*

Madhu Sudan

*Massachusetts Institute of Technology, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Moshe Y. Vardi

*Rice University, Houston, TX, USA*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

Frank S. de Boer   Marcello M. Bonsangue  
Susanne Graf   Willem-Paul de Roever (Eds.)

# Formal Methods for Components and Objects

4th International Symposium, FMCO 2005  
Amsterdam, The Netherlands, November 1-4, 2005  
Revised Lectures

## Volume Editors

Frank S. de Boer  
Centre for Mathematics and Computer Science, CWI  
Kruislaan 413, 1098 SJ Amsterdam, The Netherlands  
E-mail: F.S.de.Boer@cwi.nl

Marcello M. Bonsangue  
Leiden University  
Leiden Institute of Advanced Computer Science  
P. O. Box 9512, 2300 RA Leiden, The Netherlands  
E-mail: marcello@liacs.nl

Susanne Graf  
VERIMAG  
2 Avenue de Vignate, Centre Equitation, 38610 Grenoble-Gières, France  
E-mail: Susanne.Graf@imag.fr

Willem-Paul de Roever  
University of Kiel  
Institute of Computer Science and Applied Mathematics  
Hermann-Rodewald-Str. 3, 24118 Kiel, Germany  
E-mail: wpr@informatik.uni-kiel.de

Library of Congress Control Number: 2006930291

CR Subject Classification (1998): D.2, D.3, F.3, D.4

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN	0302-9743
ISBN-10	3-540-36749-7 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-36749-9 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 is a part of Springer Science+Business Media  
springer.com

© Springer-Verlag Berlin Heidelberg 2006  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper      SPIN: 11804192      06/3142      5 4 3 2 1 0

# Preface

Large and complex software systems provide the necessary infrastructure in all industries today. In order to construct such large systems in a systematic manner, the focus in the development methodologies has switched in the last two decades from functional issues to structural issues: both data and functions are encapsulated into software units which are integrated into large systems by means of various techniques supporting reusability and modifiability. This encapsulation principle is essential to both the object-oriented and the more recent component-based software engineering paradigms.

Formal methods have been applied successfully to the verification of medium-sized programs in protocol and hardware design. However, their application to the development of large systems requires more emphasis on specification, modeling and validation techniques supporting the concepts of reusability and modifiability and their implementation in new extensions of existing programming languages like Java.

The new format of FMCO 2005 consisted of invited keynote lectures and tutorial lectures selected through a corresponding open call. The latter provide a tutorial perspective on recent developments. In contrast to existing conferences, about half of the program consisted of invited keynote lectures by top researchers sharing their interest in the application or development of formal methods for large-scale software systems (object or component oriented). FMCO does not focus on specific aspects of the use of formal methods, but rather it aims at a systematic and comprehensive account of the expanding body of knowledge on modern software systems.

This volume contains the contributions submitted after the symposium by both invited and selected lecturers. The proceedings of FMCO 2002, FMCO 2003, and FMCO 2004 have already been published as volumes 2852, 3188, and 3657 of Springer's *Lecture Notes in Computer Science*. We believe that these proceedings provide a unique combination of ideas on software engineering and formal methods which reflect the expanding body of knowledge on modern software systems.

June 2006

F.S. de Boer  
M.M. Bonsangue  
S. Graf  
W.-P. de Roever

# Organization

The FMCO symposia are organized in the context of the project Mobi-J, a project founded by a bilateral research program of The Dutch Organization for Scientific Research (NWO) and the Central Public Funding Organization for Academic Research in Germany (DFG). The partners of the Mobi-J projects are: the Centrum voor Wiskunde en Informatica, the Leiden Institute of Advanced Computer Science, and the Christian-Albrechts-Universität Kiel.

This project aims at the development of a programming environment which supports component-based design and verification of Java programs annotated with assertions. The overall approach is based on an extension of the Java language with a notion of component that provides for the encapsulation of its internal processing of data and composition in a network by means of mobile asynchronous channels.

## Sponsoring Institutions

The Dutch Organization for Scientific Research (NWO)

The Royal Netherlands Academy of Arts and Sciences (KNAW)

The Dutch Institute for Programming research and Algorithmics (IPA)

The Centrum voor Wiskunde en Informatica (CWI), The Netherlands

The Leiden Institute of Advanced Computer Science (LIACS), The Netherlands

# Table of Contents

## Component and Service Oriented Computing

A Software Component Model and Its Preliminary Formalisation <i>Kung-Kiu Lau, Mario Ornaghi, Zheng Wang</i> .....	1
Synchronised Hyperedge Replacement as a Model for Service Oriented Computing <i>Gian Luigi Ferrari, Dan Hirsch, Ivan Lanese, Ugo Montanari, Emilio Tuosto</i> .....	22

## System Design

Control of Modular and Distributed Discrete-Event Systems <i>Jan Komenda, Jan H. van Schuppen</i> .....	44
Model-Based Security Engineering with UML: Introducing Security Aspects <i>Jan Jürjens</i> .....	64
The Pragmatics of STAIRS <i>Ragnhild Kibro Runde, Øystein Haugen, Ketil Stølen</i> .....	88

## Tools

Smallfoot: Modular Automatic Assertion Checking with Separation Logic <i>Josh Berdine, Cristiano Calcagno, Peter W. O'Hearn</i> .....	115
Orion: High-Precision Methods for Static Error Analysis of C and C++ Programs <i>Dennis R. Dams, Kedar S. Namjoshi</i> .....	138

## Algebraic Methods

Beyond Bisimulation: The “up-to” Techniques <i>Davide Sangiorgi</i> .....	161
Separation Results Via Leader Election Problems <i>Maria Grazia Vigliotti, Iain Phillips, Catuscia Palamidessi</i> .....	172

Divide and Congruence: From Decomposition of Modalities to  
Preservation of Branching Bisimulation

*Wan Fokkink, Rob van Glabbeek, Paulien de Wind* ..... 195

## Model Checking

Abstraction and Refinement in Model Checking

*Orna Grumberg* ..... 219

Program Compatibility Approaches

*Edmund Clarke, Natasha Sharygina, Nishant Sinha* ..... 243

Cluster-Based LTL Model Checking of Large Systems

*Jiří Barnat, Luboš Brim, Ivana Černá* ..... 259

Safety and Liveness in Concurrent Pointer Programs

*Dino Distefano, Joost-Pieter Katoen, Arend Rensink* ..... 280

## Assertional Methods

Modular Specification of Encapsulated Object-Oriented Components

*Arnd Poetzsch-Heffter, Jan Schäfer* ..... 313

Beyond Assertions: Advanced Specification and Verification with JML  
and ESC/Java2

*Patrice Chalin, Joseph R. Kiniry, Gary T. Leavens, Erik Poll* ..... 342

Boogie: A Modular Reusable Verifier for Object-Oriented Programs

*Mike Barnett, Bor-Yuh Evan Chang, Robert DeLine, Bart Jacobs,  
K. Rustan M. Leino* ..... 364

## Quantitative Analysis

On a Probabilistic Chemical Abstract Machine and the Expressiveness  
of Linda Languages

*Alessandra Di Pierro, Chris Hankin, Herbert Wiklicky* ..... 388

Partial Order Reduction for Markov Decision Processes: A Survey

*Marcus Groesser, Christel Baier* ..... 408

**Author Index** ..... 429