

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

Jin Song Dong Huibiao Zhu (Eds.)

Formal Methods and Software Engineering

12th International Conference
on Formal Engineering Methods, ICFEM 2010
Shanghai, China, November 17-19, 2010
Proceedings



Springer

Volume Editors

Jin Song Dong
National University of Singapore
School of Computing, Computer Science Dept.
13 Computing Drive, Singapore 117417, Singapore
E-mail: dongjs@comp.nus.edu.sg

Huibiao Zhu
East China Normal University
Software Engineering Institute
3663 Zhongshan Road (North), Shanghai, 200062, China
E-mail: hbzhu@sei.ecnu.edu.cn

Library of Congress Control Number: 2010938033

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

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN	0302-9743
ISBN-10	3-642-16900-7 Springer Berlin Heidelberg New York
ISBN-13	978-3-642-16900-7 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 2010
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 methods have made significant progress in recent years with successful stories from Microsoft (SLAM project), Intel (i7 processor verification) and NICTA/OK-Lab (formal verification of an OS kernel). The main focus of formal engineering methods lies in how formal methods can be effectively integrated into mainstream software engineering. Various advanced theories, techniques and tools have been proposed, developed and applied in the specification, design and verification of software or in the construction of software. The challenge now is how to integrate them into engineering development processes to effectively deal with large-scale and complex computer systems for their correct and efficient construction and maintenance. This requires us to improve the state of the art by researching effective approaches and techniques for integration of formal methods into industrial engineering practice, including new and emerging practice.

This series, International Conferences on Formal Engineering Methods, brings together those interested in the application of formal engineering methods to computer systems. This volume contains the papers presented at ICFEM 2010, the 12th International Conference on Formal Engineering Methods, held November 17–19, in Shanghai, China, in conjunction with the Third International Symposium on Unifying Theories of Programming (UTP 2010).

The Program Committee received 114 submissions from 29 countries and regions. Each paper was reviewed by at least three program committee members. After extensive discussion, the Program Committee decided to accept 42 papers for presentation, leaving many good-quality papers behind. We owe a great deal to the members of Program Committee and external reviewers. The program also included three invited talks by Matthew Dwyer from the University of Nebraska-Lincoln, Kokichi Futatsugi from Japan Advanced Institute of Science and Technology and Wang Yi from Uppsala University.

ICFEM 2010 was organized by the Software Engineering Institute, East China Normal University. We would like to express our sincere thanks to the staff members and students for their organizational assistance, in particular Geguang Pu, Jian Guo, Min Zhang, Qin Li and Mengying Wang. The EasyChair system was used to manage the submissions, reviewing, paper selection, and proceedings production. We would like to thank the EasyChair team for a very useful tool.

November 2010

Jin Song Dong
Huibiao Zhu

Conference Organization

Steering Committee

Keijiro Araki
Jin Song Dong
Chris George
Jifeng He
Mike Hinchey
Shaoying Liu (Chair)
John McDermid
Tetsuo Tamai
Jim Woodcock

Conference Chair

Jifeng He

Program Chairs

Jin Song Dong
Huibiao Zhu

Program Committee

Yamine Ait Ameer
Nazareno Aguirre
Bernhard Aichernig
Keijiro Araki
Farhad Arbab
Richard Banach
Jonathan Bowen
Karin Breitman
Michael Butler
Andrew Butterfield
Ana Cavalcanti
Chunqing Chen
Mingsong Chen
Wei-Ngan Chin
Jim Davies
Zhenghua Duan
Colin Fidge

John Fitzgerald
Joaquim Gabarro
Stefania Gnesi
Mike Hinchey
Thierry Jeron
Gerwin Klein
Kim Larsen
Michael Leuschel
Xuandong Li
Zhiming Liu
Shaoying Liu
Brendan Mahony
Tom Maibaum
Tiziana Margaria
Dominique Mery
Huaikou Miao
Flemming Nielson

Jun Pang
Geguang Pu
Shengchao Qin
Zongyan Qiu
Anders P. Ravn
Augusto Sampaio
Marjan Sirjani
Graeme Smith
Jing Sun
Jun Sun
Kenji Taguchi

Yih-Kuen Tsay
T.H. Tse
Sergiy Vilkomir
Xu Wang
Ji Wang
Hai Wang
Heike Wehrheim
Jim Woodcock
Wang Yi
Jian Zhang

Local Organization

Jian Guo, Qin Li, Geguang Pu (Chair), Min Zhang

Webmaster

Mengying Wang

External Reviewers

Nuno Amalio
June Andronick
Thomas Bøgholm
Granville Barnett
Lei Bu
Josep Carmona
Valentin Cassano
Pablo Castro
Shengbo Chen
Yu-Fang Chen
Zhenbang Chen
Robert Clarisó
John Colley
Phan Cong-Vinh
Marcio Cornelio
Andreea Costea
Florin Craciun
Kriangsak Damchoom
Jordi Delgado
Yuxin Deng
Brijesh Dongol
Andrew Edmunds

Alessandro Fantechi
Gianluigi Ferrari
Marc Fontaine
Cristian Gherghina
Paul Gibson
Jian Guo
Henri Hansen
Ian J. Hayes
Guanhua He
Elisabeth Jöbstl
Sven Jacobs
Mohammad Mahdi Jaghoori
Ryszard Janicki
Li Jiao
Jorge Julvez
Narges Khakpour
Ramtin Khosravi
Rafal Kolanski
Willibald Krenn
Shigeru Kusakabe
Bixin Li
Jianwen Li

Qin Li
Xiaoshan Li
Sheng Liu
Michele Loreti
Chenguang Luo
Mingsong Lv
Abdul Rahman Mat
Franco Mazzanti
Lijun Mei
Hiroschi Mochio
Charles Morisset
Alexandre Mota
Toby Murray
Benaissa Nazim
Sidney Nogueira
Ulrik Nyman
Kazuhiro Ogata
Joseph Okika
Yoichi Omori
Fernando Orejas
David Parker
Richard Payne
German Regis
Hideki Sakurada
Martin Schäf
Thomas Sewell

K.C. Shashidhar
Neeraj Singh
Jiri Srba
Kohei Suenaga
Tian Huat Tan
Claus Thrane
Ming-Hsien Tsai
Saleem Vighio
Shuling Wang
Xi Wang
Zheng Wang
Liu Wanwei
Kirsten Winter
Tobias Wrigstad
Zhongxing Xu
Shaofa Yang
Yu Yang
Fang Yu
Hongwei Zeng
Chenyi Zhang
Shaojie Zhang
Xian Zhang
Jianhua Zhao
Liang Zhao
Manchun Zheng

Table of Contents

Invited Talks

Fostering Proof Scores in CafeOBJ	1
<i>Kokichi Futatsugi</i>	
Exploiting Partial Success in Applying Automated Formal Methods (Abstract)	21
<i>Matthew B. Dwyer</i>	
Multicore Embedded Systems: The Timing Problem and Possible Solutions (Abstract)	22
<i>Wang Yi</i>	

Theorem Proving and Decision Procedures

Applying PVS Background Theories and Proof Strategies in Invariant Based Programming	24
<i>Johannes Eriksson and Ralph-Johan Back</i>	
Proof Obligation Generation and Discharging for Recursive Definitions in VDM	40
<i>Augusto Ribeiro and Peter Gorm Larsen</i>	
Correct-by-Construction Model Transformations from Partially Ordered Specifications in Coq	56
<i>Iman Poernomo and Jeffrey Terrell</i>	
Decision Procedures for the Temporal Verification of Concurrent Lists	74
<i>Alejandro Sánchez and César Sánchez</i>	
An Improved Decision Procedure for Propositional Projection Temporal Logic	90
<i>Zhenhua Duan and Cong Tian</i>	

Web Services and Workflow

A Semantic Model for Service Composition with Coordination Time Delays	106
<i>Natallia Kokash, Behnaz Changizi, and Farhad Arbab</i>	
Compensable WorkFlow Nets	122
<i>Fazle Rabbi, Hao Wang, and Wendy MacCaull</i>	

Automatically Testing Web Services Choreography with Assertions	138
<i>Lei Zhou, Jing Ping, Hao Xiao, Zheng Wang, Geguang Pu, and Zuohua Ding</i>	

Applying Ordinary Differential Equations to the Performance Analysis of Service Composition	155
<i>Zuohua Ding, Hui Shen, and Jing Liu</i>	

Verification I

Verifying Heap-Manipulating Programs with Unknown Procedure Calls	171
<i>Shengchao Qin, Chenguang Luo, Guanhua He, Florin Craciun, and Wei-Ngan Chin</i>	

API Conformance Verification for Java Programs	188
<i>Xin Li, H. James Hoover, and Piotr Rudnicki</i>	

Assume-Guarantee Reasoning with Local Specifications	204
<i>Alessio Lomuscio, Ben Strulo, Nigel Walker, and Peng Wu</i>	

Automating Coinduction with Case Analysis	220
<i>Eugen-Ioan Goriac, Dorel Lucanu, and Grigore Roşu</i>	

Applications of Formal Methods

Enhanced Semantic Access to Formal Software Models	237
<i>Hai H. Wang, Danica Damjanovic, and Jing Sun</i>	

Making Pattern- and Model-Based Software Development More Rigorous	253
<i>Denis Hatebur and Maritta Heisel</i>	

Practical Parameterised Session Types	270
<i>Andi Bejleri</i>	

A Formal Verification Study on the Rotterdam Storm Surge Barrier	287
<i>Ken Madlener, Sjaak Smetsters, and Marko van Eekelen</i>	

Verification II

Formalization and Correctness of the PALS Architectural Pattern for Distributed Real-Time Systems	303
<i>José Meseguer and Peter Csaba Ölveczky</i>	

Automated Multiparameterised Verification by Cut-Offs	321
<i>Antti Siirtola</i>	

Automating Cut-off for Multi-parameterized Systems	338
<i>Youssef Hanna, David Samuelson, Samik Basu, and Hridayesh Rajan</i>	
Method for Formal Verification of Soft-Error Tolerance Mechanisms in Pipelined Microprocessors	355
<i>Miroslav N. Velev and Ping Gao</i>	
Formal Verification of Tokeneer Behaviours Modelled in fUML Using CSP	371
<i>Islam Abdelhalim, James Sharp, Steve Schneider, and Helen Treharne</i>	

Probability and Concurrency

Model Checking Hierarchical Probabilistic Systems	388
<i>Jun Sun, Songzheng Song, and Yang Liu</i>	
Trace-Driven Verification of Multithreaded Programs	404
<i>Zijiang Yang and Kareem Sakallah</i>	
Closed Form Approximations for Steady State Probabilities of a Controlled Fork-Join Network	420
<i>Jonathan Billington and Guy Edward Gallasch</i>	
Reasoning about Safety and Progress Using Contracts	436
<i>Imene Ben-Hafaiedh, Susanne Graf, and Sophie Quinton</i>	

Program Analysis

Abstract Program Slicing: From Theory towards an Implementation . . .	452
<i>Isabella Mastroeni and Đurica Nikolić</i>	
Loop Invariant Synthesis in a Combined Domain	468
<i>Shengchao Qin, Guanhua He, Chenguang Luo, and Wei-Ngan Chin</i>	
Software Metrics in Static Program Analysis	485
<i>Andreas Vogelsang, Ansgar Fehnker, Ralf Huuck, and Wolfgang Reif</i>	
A Combination of Forward and Backward Reachability Analysis Methods	501
<i>Kazuhiro Ogata and Kokichi Futatsugi</i>	

Model Checking

Model Checking a Model Checker: A Code Contract Combined Approach	518
<i>Jun Sun, Yang Liu, and Bin Cheng</i>	

On Symmetries and Spotlights – Verifying Parameterised Systems	534
<i>Nils Timm and Heike Wehrheim</i>	
A Methodology for Automatic Diagnosability Analysis	549
<i>Jonathan Ezekiel and Alessio Lomuscio</i>	
Making the Right Cut in Model Checking Data-Intensive Timed Systems	565
<i>Rüdiger Ehlers, Michael Gerke, and Hans-Jörg Peter</i>	
Comparison of Model Checking Tools for Information Systems	581
<i>Marc Frappier, Benoît Fraikin, Romain Chossart, Raphaël Chane-Yack-Fa, and Mohammed Ouenzar</i>	
Object Orientation and Model Driven Engineering	
A Modular Scheme for Deadlock Prevention in an Object-Oriented Programming Model	597
<i>Scott West, Sebastian Nanz, and Bertrand Meyer</i>	
Model-Driven Protocol Design Based on Component Oriented Modeling	613
<i>Prabhu Shankar Kaliappan, Hartmut König, and Sebastian Schmerl</i>	
Laws of Pattern Composition	630
<i>Hong Zhu and Ian Bayley</i>	
Dynamic Resource Reallocation between Deployment Components	646
<i>Einar Broch Johnsen, Olaf Owe, Rudolf Schlatte, and Silvia Lizeth Tapia Tarifa</i>	
Specification and Verification	
A Pattern System to Support Refining Informal Ideas into Formal Expressions	662
<i>Xi Wang, Shaoying Liu, and Huaikou Miao</i>	
Specification Translation of State Machines from Equational Theories into Rewrite Theories	678
<i>Min Zhang, Kazuhiro Ogata, and Masaki Nakamura</i>	
Alternating Interval Based Temporal Logics	694
<i>Cong Tian and Zhenhua Duan</i>	
Author Index	711