Lecture Notes in Computer Science 6447

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

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 Ameur
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
Swen 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
Hiroshi 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

Theorem Proving and Decision Procedures

Web Services and Workflow

Verification I

Applications of Formal Methods

Verification II

Probability and Concurrency

Program Analysis

Model Checking

Object Orientation and Model Driven Engineering

Specification and Verification