

*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*

Toshiaki Aoki Kenji Taguchi (Eds.)

# Formal Methods and Software Engineering

14th International Conference  
on Formal Engineering Methods, ICFEM 2012  
Kyoto, Japan, November 12-16, 2012  
Proceedings



Springer

Volume Editors

Toshiaki Aoki

Japan Advanced Institute of Science and Technology (JAIST)

1-1, Asahidai, Nomi, Ishikawa 923-1292, Japan

E-mail: toshiaki@jaist.ac.jp

Kenji Taguchi

National Institute of Advanced Industrial Science and Technology (AIST)

Nakoji 3-11-46, Amagasaki, Hyogo 661-0974, Japan

E-mail: kenji.taguchi@aist.go.jp

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-34280-6

e-ISBN 978-3-642-34281-3

DOI 10.1007/978-3-642-34281-3

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012949358

CR Subject Classification (1998): D.2.4, D.2, D.3, F.3, F.4.1, C.2, C.2.4

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© Springer-Verlag Berlin Heidelberg 2012

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

*Typesetting:* Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

# Preface

The aim of the International Conference on Formal Engineering Methods (ICFEM) is to provide an international forum to discuss research issues in formal methods as well as to bring practitioners and researchers together to further develop and to apply them to real-world problems. Formal methods are now being used in wide range of industrial sectors, and particularly in safety-critical areas such as railways, automobiles, and avionics. We hope that ICFEM plays an important role in encouraging researchers not only to advance theories but also to develop application techniques of formal methods.

This was the 14th conference in the series and the third time that it was held in Japan. It has been over a year since the Great East Japan earthquake and Fukushima nuclear disaster took place. We really appreciate the encouragement, concern, and humanitarian aid from all over the world and would like people to come and see how we quickly recovered from such a great disaster.

The Program Committee received 85 submissions from 30 countries and each paper was reviewed by at least three expert reviewers. We chose 31 papers as the result of intensive discussions held among the Program Committee members. We really appreciate the excellent reviews and lively discussions of the Program Committee members and external reviewers in the review process. This year we chose three prominent invited speakers, Mario Tokoro from Sony Computer Science Laboratories, Robert E. Shostak from Vocera Communications, Inc., and Darren Cofer from Rockwell Collins, Advanced Technology Center. The abstracts of their talks are included in these proceedings.

ICFEM 2012 was jointly organized by the National Institute of Advanced Industrial Science and Technology (AIST) and Japan Advanced Institute of Science and Technology (JAIST). This conference could not have been organized without the strong support from the staff members of both institutes. We would especially like to thank Yuki Chiba, Takashi Kitamura, Kazuhiro Ogata, Weiqiang Kong (University of Kyushu), Kenro Yadake, Hiromi Hatanaka, and Satomi Takeda for their great help in organizing the conference. We also appreciate the gentle guidance and help from General Chairs Shaoying Liu (Hosei University) and Kokichi Futatsugi and the conference chair, Hitoshi Ohsaki.

November 2012

Toshiaki Aoki  
Kenji Taguchi

# Organization

## Steering Committee

Keijiro Araki	Kyushu University, Japan
Michael Butler	University of Southampton, UK
Jin Song Dong	National University of Singapore, Singapore
Jifeng He	East China Normal University, China
Mike Hinchey	University of Limerick, Ireland
Shaoying Liu (Chair)	Hosei University, Japan
Jeff Offutt	George Mason University, USA
Shengchao Qin	University of Teesside, UK

## General Chairs

Kokichi Futatsugi	JAIST, Japan
Shaoying Liu	Hosei University, Japan

## Conference Chair

Hitoshi Ohsaki	AIST, Japan
----------------	-------------

## Program Chairs

Kenji Taguchi	AIST, Japan
Toshiaki Aoki	JAIST, Japan

## Workshop/Tutorial Chairs

Kazuhiro Ogata	JAIST, Japan
Weiqliang Kong	Kyushu University, Japan

## Publicity/Publication Chairs

Yuki Chiba	JAIST, Japan
Takashi Kitamura	AIST, Japan

## Student Volunteer Chair

Kenro Yadake	JAIST, Japan
--------------	--------------

## Web Chair

Nao Aoki JAIST, Japan

## Conference Secretaries

Hiromi Hatanaka AIST, Japan

Satomi Takeda AIST, Japan

## Program Committee

Bernhard K. Aichernig	Graz University of Technology, Austria
Cyrille Valentin Artho	AIST, Japan
Richard Banach	University of Manchester, UK
Nikolaj Bjørner	Microsoft Research Redmond, USA
Jonathan P. Bowen	Meusephile Limited and London South Bank University, UK
Michael Butler	University of Southampton, UK
Sagar Chaki	Carnegie Mellon Software Engineering Institute, USA
Rance Cleaveland	University of Maryland, USA
Jim Davies	University of Oxford, UK
Zhenhua Duan	Xidian University, China
Joaquim Garbarro	Universitat Politècnica de Catalunya, Spain
Andy Galloway	University of York, UK
Stefania Gnesi	ISTI-CNR, Italy
Wolfgang Grieskamp	Google, USA
Kim Guldstrand Larsen	Aalborg University, Denmark
Klaus Havelund	NASA JPL, California Institute of Technology, USA
Daniel Jackson	MIT, USA
Thierry Jéron	INRIA Rennes, France
Gerwin Klein	NICTA and University of New South Wales, Australia
Weiqliang Kong	Kyushu University, Japan
Peter Gorm Larsen	Aarhus University, Denmark
Insup Lee	University of Pennsylvania, USA
Michael Leuschel	University of Düsseldorf, Germany
Xuandong Li	Nanjing University, China
Yuan-Fang Li	Monash University, Australia
Zhiming Liu	United Nations University, Macao
Dominique Méry	Université de Lorraine, France

Stephan Merz	INRIA Research Center Nancy Grand-Est, France
Huaikou Miao	Shanghai University, China
Alexandre Mota	Universidade Federal de Pernambuco, Brazil
Shin Nakajima	National Institute of Informatics, Japan
Kazuhiro Ogata	JAIST, Japan
Jose Oliveira	Universidade do Minho, Portugal
Jun Pang	University of Luxembourg, Luxembourg
Shengchao Qin	Teesside University, UK
Zongyan Qiu	Peking University, China
S. Ramesh	General Motors R&D, India
Alexander Romanovsky	Newcastle University, UK
Wuwei Shen	Western Michigan University, USA
Marjan Sirjani	Reykjavik University, Iceland
Graeme Smith	University of Queensland, Australia
Jing Sun	The University of Auckland, New Zealand
Jun Sun	Singapore University of Technology and Design, Singapore
Yih-Kuen Tsay	National Taiwan University, Taiwan
Viktor Vafeiadis	Max Planck Institute for Software Systems, Germany
Hai H. Wang	Aston University, UK
Ji Wang	National Laboratory for Parallel and Distributed Processing, China
Wang Yi	Uppsala University, Sweden
Jian Zhang	Chinese Academy of Sciences, China
Huibiao Zhu	East China Normal University, China

## Additional Reviewers

Ait Ameer, Yamine	Dong, Wei
Alpuente, María	Du, Dehui
Andrews, Zoe	Farias, Adalberto Cajueiro De
Andronick, June	Ferrari, Alessio
Barnett, Granville	Ferreira, Joao F.
Bryans, Jeremy	Flodin, Jonas
Bu, Lei	Fontana, Peter
Carmona, Josep	Ghassemi, Fatemeh
Chen, Liqian	Goré, Rajeev
Chen, Xin	Gui, Lin
Chen, Yu-Fang	Hasuo, Ichiro
Chen, Zhenbang	He, Guanhua
Coleman, Joey	Huang, Yanhong
Cunha, Alcino	Höfner, Peter
Daum, Matthias	Iliasov, Alexei

Iyoda, Juliano	Shi, Ling
Juhl, Line	Shu, Qin
Khakpour, Narges	Silva, Renato Alexandre
Khamespanah, Ehsan	Singh, Neeraj
Khosravi, Ramtin	Song, Songzheng
Kitamura, Takashi	Sousa Pinto, Jorge
Li, Qin	Stainer, Amelie
Lluch Lafuente, Alberto	Su, Wen
Maamria, Issam	Thomson, Jimmy
Massink, Mieke	Tounsi, Mohamed
Mazzara, Manuel	Traonouez, Louis-Marie
Melo De Sousa, Simão	Tsai, Ming-Hsien
Murray, Toby	Venkatasubramanian, Krishna K.
Nielsen, Claus Ballegaard	Wang, Bow-Yaw
Orejas, Fernando	Wang, Linzhang
Passmore, Grant	Wang, Shaohui
Petrocchi, Marinella	Wang, Zheng
Plagge, Daniel	Wu, Peng
Proenca, Jose	Xiao, Hao
Ricker, Laurie	Xu, Meng
Sabouri, Hamideh	Zhang, Chenyi
Salehi Fathabadi, Asieh	Zhang, Nan
Sanan, David	Zhang, Pengcheng
Sarshogh, Mohammad Reza	Zhang, Yufeng
Satpathy, Manoranjan	Zhao, Jianhua
Schäf, Martin	Zhong, Hao
Sharify, Zeynab	Zhu, Ping

## Sponsors

National Institute of Advanced Industrial Science and Technology (AIST), Japan  
Research Center for Software Verification, Japan Advanced Institute of Science  
and Technology (JAIST), Japan



# Table of Contents

## Invited Speech

Toward Practical Application of Formal Methods in Software Lifecycle Processes .....	1
<i>Mario Tokoro</i>	
Formal Methods in the Aerospace Industry: Follow the Money .....	2
<i>Darren Cofer</i>	
Applying Term Rewriting to Speech Recognition of Numbers .....	4
<i>Robert E. Shostak</i>	

## Concurrency

Variable Permissions for Concurrency Verification .....	5
<i>Duy-Khanh Le, Wei-Ngan Chin, and Yong-Meng Teo</i>	
A Concurrent Temporal Programming Model with Atomic Blocks .....	22
<i>Xiaoxiao Yang, Yu Zhang, Ming Fu, and Xinyu Feng</i>	
A Composable Mixed Mode Concurrency Control Semantics for Transactional Programs.....	38
<i>Granville Barnett and Shengchao Qin</i>	

## Applications of Formal Methods to New Areas

Towards a Formal Verification Methodology for Collective Robotic Systems .....	54
<i>Edmond Gjondrekaj, Michele Loreti, Rosario Pugliese, Francesco Tiezzi, Carlo Pinciroli, Manuele Brambilla, Mauro Birattari, and Marco Dorigo</i>	
Modeling Resource-Aware Virtualized Applications for the Cloud in Real-Time ABS .....	71
<i>Einar Broch Johnsen, Rudolf Schlatte, and Silvia Lizeth Tapia Tarifa</i>	
Specification and Model Checking of the Chandy and Lamport Distributed Snapshot Algorithm in Rewriting Logic .....	87
<i>Kazuhiro Ogata and Phan Thi Thanh Huyen</i>	

## Quantity and Probability

Quantitative Program Dependence Graphs . . . . .	103
<i>Chunyan Mu</i>	
Quantitative Analysis of Information Flow Using Theorem Proving . . . . .	119
<i>Tarek Mhamdi, Osman Hasan, and Sofiène Tahar</i>	
Modeling and Verification of Probabilistic Actor Systems Using pRebeca . . . . .	135
<i>Mahsa Varshosaz and Ramtin Khosravi</i>	

## Formal Verification

Modular Verification of OO Programs with Interfaces . . . . .	151
<i>Qiu Zongyan, Hong Ali, and Liu Yijing</i>	
Separation Predicates: A Taste of Separation Logic in First-Order Logic . . . . .	167
<i>François Bobot and Jean-Christophe Filliâtre</i>	
The Confinement Problem in the Presence of Faults . . . . .	182
<i>William L. Harrison, Adam Procter, and Gerard Allwein</i>	

## Modeling and Development Methodology

Verification of ATL Transformations Using Transformation Models and Model Finders . . . . .	198
<i>Fabian Büttner, Marina Egea, Jordi Cabot, and Martin Gogolla</i>	
Automatic Generation of Provably Correct Embedded Systems . . . . .	214
<i>Shang-Wei Lin, Yang Liu, Pao-Ann Hsiung, Jun Sun, and Jin Song Dong</i>	
Complementary Methodologies for Developing Hybrid Systems with Event-B . . . . .	230
<i>Wen Su, Jean-Raymond Abrial, and Huibiao Zhu</i>	

## Temporal Logics

A Temporal Logic with Mean-Payoff Constraints . . . . .	249
<i>Takashi Tomita, Shin Hiura, Shigeki Hagihara, and Naoki Yonezaki</i>	
Time Constraints with Temporal Logic Programming . . . . .	266
<i>Meng Han, Zhenhua Duan, and Xiaobing Wang</i>	
Stepwise Satisfiability Checking Procedure for Reactive System Specifications by Tableau Method and Proof System . . . . .	283
<i>Yoshinori Neya and Noriaki Yoshiura</i>	

## Abstraction and Refinement

Equational Abstraction Refinement for Certified Tree Regular Model Checking .....	299
<i>Yohan Boichut, Benoit Boyer, Thomas Genet, and Axel Legay</i>	
SMT-Based False Positive Elimination in Static Program Analysis .....	316
<i>Maximilian Junker, Ralf Huuck, Ansgar Fehnker, and Alexander Knapp</i>	
Predicate Analysis with Block-Abstraction Memoization .....	332
<i>Daniel Wonisch and Heike Wehrheim</i>	
Heuristic-Guided Abstraction Refinement for Concurrent Systems .....	348
<i>Nils Timm, Heike Wehrheim, and Mike Czech</i>	
More Anti-chain Based Refinement Checking .....	364
<i>Ting Wang, Songzheng Song, Jun Sun, Yang Liu, Jin Song Dong, Xinyu Wang, and Shanping Li</i>	

## Tools

An Analytical and Experimental Comparison of CSP Extensions and Tools .....	381
<i>Ling Shi, Yang Liu, Jun Sun, Jin Song Dong, and Gustavo Carvalho</i>	
Symbolic Model-Checking of Stateful Timed CSP Using BDD and Digitization .....	398
<i>Truong Khanh Nguyen, Jun Sun, Yang Liu, and Jin Song Dong</i>	
Annotations for Alloy: Automated Incremental Analysis Using Domain Specific Solvers .....	414
<i>Svetoslav Ganov, Sarfraz Khurshid, and Dewayne E. Perry</i>	
State Space c-Reductions of Concurrent Systems in Rewriting Logic ....	430
<i>Alberto Lluch Lafuente, José Meseguer, and Andrea Vandin</i>	

## Testing and Runtime Verification

A Practical Loop Invariant Generation Approach Based on Random Testing, Constraint Solving and Verification .....	447
<i>Mengjun Li</i>	
ConSMutate: SQL Mutants for Guiding Concolic Testing of Database Applications .....	462
<i>Tanmoy Sarkar, Samik Basu, and Johnny S. Wong</i>	

Demonic Testing of Concurrent Programs . . . . .	478
<i>Scott West, Sebastian Nanz, and Bertrand Meyer</i>	
Towards Certified Runtime Verification . . . . .	494
<i>Jan Olaf Blech, Yliès Falcone, and Klaus Becker</i>	
<b>Author Index</b> . . . . .	<b>511</b>