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
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 a 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**

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keijiro Araki</td>
<td>Kyushu University, Japan</td>
</tr>
<tr>
<td>Michael Butler</td>
<td>University of Southampton, UK</td>
</tr>
<tr>
<td>Jin Song Dong</td>
<td>National University of Singapore, Singapore</td>
</tr>
<tr>
<td>Jifeng He</td>
<td>East China Normal University, China</td>
</tr>
<tr>
<td>Mike Hinchey</td>
<td>University of Limerick, Ireland</td>
</tr>
<tr>
<td>Shaoying Liu (Chair)</td>
<td>Hosei University, Japan</td>
</tr>
<tr>
<td>Jeff Offutt</td>
<td>George Mason University, USA</td>
</tr>
<tr>
<td>Shengchao Qin</td>
<td>University of Teesside, UK</td>
</tr>
</tbody>
</table>

**General Chairs**

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kokichi Futatsugi</td>
<td>JAIST, Japan</td>
</tr>
<tr>
<td>Shaoying Liu</td>
<td>Hosei University, Japan</td>
</tr>
</tbody>
</table>

**Conference Chair**

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hitoshi Ohsaki</td>
<td>AIST, Japan</td>
</tr>
</tbody>
</table>

**Program Chairs**

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kenji Taguchi</td>
<td>AIST, Japan</td>
</tr>
<tr>
<td>Toshiaki Aoki</td>
<td>JAIST, Japan</td>
</tr>
</tbody>
</table>

**Workshop/Tutorial Chairs**

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kazuhiro Ogata</td>
<td>JAIST, Japan</td>
</tr>
<tr>
<td>Weiqiang Kong</td>
<td>Kyushu University, Japan</td>
</tr>
</tbody>
</table>

**Publicity/Publication Chairs**

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yuki Chiba</td>
<td>JAIST, Japan</td>
</tr>
<tr>
<td>Takashi Kitamura</td>
<td>AIST, Japan</td>
</tr>
</tbody>
</table>

**Student Volunteer Chair**

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kenro Yadake</td>
<td>JAIST, Japan</td>
</tr>
</tbody>
</table>
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 Museophile 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 Gabarro 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
Weiqiang 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 Ameur, Yamine  
Dong, Wei

Alpuente, Marı́a  
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
Juhl, Line
Khakpour, Narges
Khamespanah, Ehsan
Khosravi, Ramtin
Kitamura, Takashi
Li, Qin
Lluch Lafuente, Alberto
Maamria, Issam
Massink, Mieke
Mazzara, Manuel
Melo De Sousa, Simão
Murray, Toby
Nielsen, Claus Ballegaard
Orejas, Fernando
Passmore, Grant
Petrocchi, Marinella
Plagge, Daniel
Proenca, Jose
Ricker, Laurie
Sabouri, Hamideh
Salehi Fathabadi, Asieh
Sanan, David
Sarshogh, Mohammad Reza
Satpathy, Manoranjan
Schäf, Martin
Sharify, Zeynab

Shi, Ling
Shu, Qin
Silva, Renato Alexandre
Singh, Neeraj
Song, Songzheng
Sousa Pinto, Jorge
Stainer, Amelie
Su, Wen
Thomson, Jimmy
Tounsi, Mohamed
Traonouez, Louis-Marie
Tsai, Ming-Hsien
Venkatasubramanian, Krishna K.
Wang, Bow-Yaw
Wang, Linzhang
Wang, Shaohui
Wang, Zheng
Wu, Peng
Xiao, Hao
Xu, Meng
Zhang, Chenyi
Zhang, Nan
Zhang, Pengcheng
Zhang, Yufeng
Zhao, Jianhua
Zhong, Hao
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  
* Mario Tokoro  

Formal Methods in the Aerospace Industry: Follow the Money ............ 2  
* Darren Cofer  

Applying Term Rewriting to Speech Recognition of Numbers .......... 4  
* Robert E. Shostak  

## Concurrency

Variable Permissions for Concurrency Verification ................. 5  
* Duy-Khanh Le, Wei-Ngan Chin, and Yong-Meng Teo  

A Concurrent Temporal Programming Model with Atomic Blocks ...... 22  
* Xiaoxiao Yang, Yu Zhang, Ming Fu, and Xinyu Feng  

A Composable Mixed Mode Concurrency Control Semantics  
for Transactional Programs .................................................. 38  
* Granville Barnett and Shengchao Qin  

## Applications of Formal Methods to New Areas

Towards a Formal Verification Methodology for Collective Robotic Systems ........................................ 54  
* Edmond Gjondrekaj, Michele Loreti, Rosario Pugliese,  
  Francesco Tiezzi, Carlo Pincioli, Manuele Brambilla,  
  Mauro Birattari, and Marco Dorigo  

Modeling Resource-Aware Virtualized Applications for the Cloud in Real-Time ABS .................................. 71  
* Einar Broch Johnsen, Rudolf Schlatte, and Silvia Lizeth Tapia Tarifa  

Specification and Model Checking of the Chandy and Lamport Distributed Snapshot Algorithm in Rewriting Logic ............. 87  
* Kazuhiro Ogata and Phan Thi Thanh Huyen
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Quantity and Probability</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantitative Program Dependence Graphs</td>
<td>103</td>
</tr>
<tr>
<td></td>
<td>Chunyan Mu</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quantitative Analysis of Information Flow Using Theorem Proving</td>
<td>119</td>
</tr>
<tr>
<td></td>
<td>Tarek Mhamdi, Osman Hasan, and Sofiène Tahar</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Modeling and Verification of Probabilistic Actor Systems Using</td>
<td>135</td>
</tr>
<tr>
<td></td>
<td>pRebeca</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mahsa Varshosaz and Ramtin Khosravi</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Formal Verification</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Modular Verification of OO Programs with Interfaces</td>
<td>151</td>
</tr>
<tr>
<td></td>
<td>Qiu Zongyan, Hong Ali, and Liu Yijing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Separation Predicates: A Taste of Separation Logic in First-Order Logic</td>
<td>167</td>
</tr>
<tr>
<td></td>
<td>François Bobot and Jean-Christophe Filliâtre</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Confinement Problem in the Presence of Faults</td>
<td>182</td>
</tr>
<tr>
<td></td>
<td>William L. Harrison, Adam Procter, and Gerard Allwein</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Modeling and Development Methodology</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verification of ATL Transformations Using Transformation Models and Model Finders</td>
<td>198</td>
</tr>
<tr>
<td></td>
<td>Fabian Büttner, Marina Egea, Jordi Cabot, and Martin Gogolla</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Automatic Generation of Provably Correct Embedded Systems</td>
<td>214</td>
</tr>
<tr>
<td></td>
<td>Shang-Wei Lin, Yang Liu, Pao-Ann Hsiung, Jun Sun, and Jin Song Dong</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Complementary Methodologies for Developing Hybrid Systems</td>
<td>230</td>
</tr>
<tr>
<td></td>
<td>Wen Su, Jean-Raymond Abrial, and Huibiao Zhu</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Temporal Logics</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A Temporal Logic with Mean-Payoff Constraints</td>
<td>249</td>
</tr>
<tr>
<td></td>
<td>Takashi Tomita, Shin Hiura, Shigeki Hagihara, and Naoki Yonezaki</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time Constraints with Temporal Logic Programming</td>
<td>266</td>
</tr>
<tr>
<td></td>
<td>Meng Han, Zhenhua Duan, and Xiaobing Wang</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stepwise Satisfiability Checking Procedure for Reactive System</td>
<td>283</td>
</tr>
<tr>
<td></td>
<td>Yoshinori Neya and Noriaki Yoshiura</td>
<td></td>
</tr>
</tbody>
</table>
## Abstraction and Refinement

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

## Tools

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

## Testing and Runtime Verification

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Practical Loop Invariant Generation Approach Based on Random Testing, Constraint Solving and Verification</td>
<td>447</td>
</tr>
<tr>
<td>Mengjun Li</td>
<td></td>
</tr>
<tr>
<td>ConSMutate: SQL Mutants for Guiding Concolic Testing of Database Applications</td>
<td>462</td>
</tr>
<tr>
<td>Tanmoy Sarkar, Samik Basu, and Johnny S. Wong</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Demonic Testing of Concurrent Programs</td>
<td>478</td>
</tr>
<tr>
<td><em>Scott West, Sebastian Nanz, and Bertrand Meyer</em></td>
<td></td>
</tr>
<tr>
<td>Towards Certified Runtime Verification</td>
<td>494</td>
</tr>
<tr>
<td><em>Jan Olaf Blech, Yliès Falcone, and Klaus Becker</em></td>
<td></td>
</tr>
<tr>
<td><strong>Author Index</strong></td>
<td>511</td>
</tr>
</tbody>
</table>