

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

New York University, NY, 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

Jim Davies Wolfram Schulte
Mike Barnett (Eds.)

Formal Methods and Software Engineering

6th International Conference
on Formal Engineering Methods, ICFEM 2004
Seattle, WA, USA, November 8-12, 2004
Proceedings



Springer

Volume Editors

Jim Davies

University of Oxford, Software Engineering Programme

Wolfson Building, Parks Road, Oxford OX1 3QD, UK

E-mail: jim.davies@comlab.ox.ac.uk

Wolfram Schulte

Mike Barnett

Microsoft Research

One Microsoft Way, Cedar Court 113/4048, Redmond, WA 98052-6399, USA

E-mail: {schulte, mbarnett}@microsoft.com

Library of Congress Control Number: 2004114617

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

ISSN 0302-9743

ISBN 3-540-23841-7 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 is a part of Springer Science+Business Media

springeronline.com

© Springer-Verlag Berlin Heidelberg 2004

Printed in Germany

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

Printed on acid-free paper SPIN: 11348801 06/3142 5 4 3 2 1 0

Preface

Formal engineering methods are changing the way that software systems are developed. With language and tool support, they are being used for automatic code generation, and for the automatic abstraction and checking of implementations. In the future, they will be used at every stage of development: requirements, specification, design, implementation, testing, and documentation.

The ICFEM series of conferences aims to bring together those interested in the application of formal engineering methods to computer systems. Researchers and practitioners, from industry, academia, and government, are encouraged to attend, and to help advance the state of the art. Authors are strongly encouraged to make their ideas as accessible as possible, and there is a clear emphasis upon work that promises to bring practical, tangible benefit: reports of case studies should have a conceptual message, theory papers should have a clear link to application, and papers describing tools should have an account of results.

ICFEM 2004 was the sixth conference in the series, and the first to be held in North America. Previous conferences were held in Singapore, China, UK, Australia, and Japan. The Programme Committee received 110 papers and selected 30 for presentation. The final versions of those papers are included here, together with 2-page abstracts for the 5 accepted tutorials, and shorter abstracts for the 4 invited talks.

We would like to thank: Dines Bjørner, for his work in organizing speakers and sponsors; Jin Song Dong and Jim Woodcock, for an excellent handover from ICFEM 2003; Joxan Jaffar, J Strother Moore, Peter Neumann, and Amitabh Srivastava, for agreeing to address the conference; the authors, for submitting their work; the Programme Committee, and their colleagues, for their reviews; and Springer, for their help with publication.

ICFEM 2004 was organized by Microsoft Research in Seattle, with additional support and sponsorship from the University of Oxford, the United Nations University, Formal Methods Europe, NASA, and ORA Canada.

November 2004

Jim Davies
Wolfram Schulte
Mike Barnett

Organizing Committee

Conference Committee

Mike Barnett (Microsoft Research, USA)

Local Organization

Dines Bjørner (National University of Singapore, Singapore)

Conference Chair

Jim Davies (University of Oxford, UK)

Programme Co-chair

Wolfram Schulte (Microsoft Research, USA)

Programme Co-chair

Hongjun Zheng (Semantics Design, USA)

Workshops and Tutorials Chair

Sponsors

Microsoft Research

www.research.microsoft.com

Oxford University Software Engineering Programme

www.softeng.ox.ac.uk

United Nations University–International Institute for Software Technology

www.iist.unu.edu

Formal Methods Europe (FME)

www.fmeurope.org

NASA–JPL Laboratory for Reliable Software

eis.jpl.nasa.gov/lars/

ORA Canada

www.ora.on.ca

Steering Committee

Keiji Araki (Kyushu University, Japan)

Jin Song Dong (National University of Singapore, Singapore)

Chris George (United Nations University, Macau)

Jifeng He (*Chair*) (IIST, United Nations University, Macau)

Mike Hinchey (NASA, USA)

Shaoying Liu (Hosei University, Japan)

John McDermid (University of York, UK)

Tetsuo Tamai (University of Tokyo, Japan)

Jim Woodcock (University of York, UK)

Programme Committee

Adnan Aziz (University of Texas, USA)
Richard Banach (University of Manchester, UK)
Egon Börger (University of Pisa, Italy)
Jonathan Bowen (London South Bank University, UK)
Manfred Broy (University of Munich, Germany)
Michael Butler (University of Southampton, UK)
Ana Cavalcanti (University of Kent, UK)
Dan Craigen (ORA, Canada)
Jin Song Dong (National University of Singapore, Singapore)
Matthew Dwyer (Kansas State University, USA)
John Fitzgerald (University of Newcastle upon Tyne, UK)
David Garlan (Carnegie Mellon University, Pittsburgh, USA)
Thomas Jensen (IRISA/CNRS Campus de Beaulieu, Rennes, France)
Jim Larus (Microsoft Research, USA)
Mark Lawford (McMaster University, Canada)
Huimin Lin (Chinese Academy of Sciences, Beijing, China)
Peter Lindsay (University of Queensland, Australia)
Shaoying Liu (Hosei University, Japan)
Zhiming Liu (United Nations University, Macau SAR, China)
Brendan Mahony (Department of Defence, Australia)
Marc Frappier (Université de Sherbrooke, Québec, Canada)
William Bradley Martin (National Security Agency, USA)
David Notkin (University of Washington, USA)
Jeff Offutt (George Mason University, USA)
Harald Ruess (Computer Science Laboratory, SRI, USA)
Augusto Sampaio (Universidade Federal de Pernambuco, Brazil)
Thomas Santen (Technical University of Berlin, Germany)
Doug Smith (Kestrel Institute, USA)
Graeme Smith (University of Queensland, Australia)
Paul A. Swatman (University of South Australia, Australia)
Sofiene Tahar (Concordia University, Canada)
T.H. Tse (Hong Kong University, Hong Kong)
Yi Wang (Uppsala University, Sweden)
Farn Wang (National Taiwan University, Taiwan)
Jeannette Wing (Carnegie Mellon University, USA)
Jim Woodcock (University of York, UK)

Reviewers

Amr Abdel-Hamid; Isaam Al-azzoni; Adnan Aziz; Richard Banach;
Andreas Bauer; Jounaidi Ben Hassen; Egon Börger; Jonathan Bowen;
Peter Braun; Manfred Broy; Michael Butler; Colin Campbell; Ana Cavalcanti;
Alessandra Cavarra; Antonio Cerone; Yifeng Chen; Corina Cirstea;
David Clark; Dan Craigen; Charles Crichton; Jim Davies; Roger Duke;
Bruno Dutertre; Matthew Dwyer; Pao-Ann Eric Hsiung; Yuan Fang Li;
Bill Farmer; William M. Farmer; Carla Ferreira; Colin Fidge; John Fitzgerald;
Marc Frappier; Jorn Freiheit; David Garlan; Amjad Gawanmeh;
Frederic Gervais; Jeremy Gibbons; Uwe Glaesser; Andy Gravell;
Wolfgang Grieskamp; Ali Habibi; John Hakansson; Steve Harris; Jifeng He;
Maritta Heisel; Steffen Helke; Matthew Hennessy; Xiayong Hu;
Geng-Dian Huang; Chung-Yang Ric Huang; Van Hung Dang; Jiale Huo;
Cornelia P. Inggs; Jan Jürjens; Bart Jacobs; Thomas Jensen; Thierry Jeron;
Zhi Jin; Wolfram Kahl; Soon-Kyeong Kim; Soon Kyeong Kim; Leonid Kof;
Pushmeet Kohli; Pavel Krcal; Sy-Yen Kuo; Rom Langerak; James Larus;
Mark Lawford; Ryan Leduc; Karl Lermer; Guangyuan Li; Xiaoshan Li;
Huimin Lin; Peter Lindsay; Shaoying Liu; Zhiming Liu; Quan Long;
Marcio Lopes Cornelio; Dorel Lucanu; Anthony MacDonald; Brendan Mahony;
William Bradley Martin; Jim McCarthy; M. Meisinger; Yassine Mokhtari;
Leonid Mokrushin; Alexandre Mota; Muan Yong Ng; Sidney Nogueira;
David Notkin; Jeff Offutt; Chun Ouyang; Hong Pan; Jun Pang;
Paul Pettersson; Mike Poppleton; Steven Postma; Stephane Lo Presti;
Wolfgang Reisig; Abdolbaghi Rezazadeh; River; Harald Ruess; Heinrich Rust;
Vlad Rusu; Augusto Sampaio; Thomas Santen; Renate Schmidt;
Wolfram Schulte; Thorsten Schutt; Dirk Seifert; Laura Semini; Adnan Sherif;
Benjamin Sigonneau; Carlo Simon; Andrew Simpson; Doug Smith;
Graeme Smith; Doug Smith; Colin Snook; Jin Song Dong; Maria Sorea;
Mark Staples; Jun Sun; Paul A. Swatman; Sofiene Tahar; J.P. Talpin;
Rodrigo Teixeira Ramos; Nikolai Tillmann; T.H. Tse; Phillip J. Turner;
Margus Veanes; S. Vogel; Philip Wadler; Farn Wang; Bow-Yaw Wang;
Alan Wassying; Jun Wei; Guido Wimmel; Jeannette Wing; Kirsten Winter;
Jim Woodcock; Wang Yi; Fang Yu; Mohamed Zaki; Wenhui Zhang;
Guangquan Zhang; Ning Zhang; Riley Zheng; Xiaocong Zhou; Jeff Zucker

Table of Contents

Tutorials

Model-Based Development: Combining Engineering Approaches and Formal Techniques <i>Bernhard Schätz</i>	1
Tutorial on the RAISE Language, Method and Tools <i>Chris George</i>	3
Model-Based Testing with Spec# <i>Jonathan Jacky</i>	5
Formal Engineering for Industrial Software Development – An Introduction to the SOFL Specification Language and Method <i>Shaoying Liu</i>	7
Tutorial: Software Model Checking <i>Edmund Clarke, Daniel Kroening</i>	9

Invited Talks

Engineering Quality Software <i>Amitabh Srivastava</i>	11
When Can Formal Methods Make a Real Difference? <i>Peter G. Neumann</i>	12
On the Adoption of Formal Methods by Industry: The ACL2 Experience <i>J Strother Moore</i>	13
A CLP Approach to Modelling Systems <i>Joxan Jaffar</i>	14

Full Papers

Multi-prover Verification of C Programs <i>Jean-Christophe Filliâtre, Claude Marché</i>	15
Memory-Model-Sensitive Data Race Analysis <i>Yue Yang, Ganesh Gopalakrishnan, Gary Lindstrom</i>	30
Formal Models for Web Navigations with Session Control and Browser Cache <i>Jessica Chen, Xiaoshan Zhao</i>	46

Managing Verification Activities Using SVM <i>Bill Aldrich, Ansgar Fehnker, Peter H. Feiler, Zhi Han, Bruce H. Krogh, Eric Lim, Shiva Sivashankar</i>	61
A General Model for Reachability Testing of Concurrent Programs <i>Richard H. Carver, Yu Lei</i>	76
A Knowledge Based Analysis of Cache Coherence <i>Kai Baukus, Ron van der Meyden</i>	99
A Propositional Logic-Based Method for Verification of Feature Models <i>Wei Zhang, Haiyan Zhao, Hong Mei</i>	115
Deriving Probabilistic Semantics Via the ‘Weakest Completion’ <i>He Jifeng, Carroll Morgan, Annabelle McIver</i>	131
CSP Representation of Game Semantics for Second-Order Idealized Algol <i>Aleksandar Dimovski, Ranko Lazić</i>	146
An Equational Calculus for Alloy <i>Marcelo F. Frias, Carlos G. López Pombo, Nazareno M. Aguirre</i>	162
Guiding Spin Simulation <i>Nicolae Goga, Judi Romijn</i>	176
Linear Inequality LTL (<i>iLTL</i>): A Model Checker for Discrete Time Markov Chains <i>YoungMin Kwon, Gul Agha</i>	194
Software Model Checking Using Linear Constraints <i>Alessandro Armando, Claudio Castellini, Jacopo Mantovani</i>	209
Counterexample Guided Abstraction Refinement Via Program Execution <i>Daniel Kroening, Alex Groce, Edmund Clarke</i>	224
Faster Analysis of Formal Specifications <i>Fabrice Bouquet, Bruno Legeard, Mark Utting, Nicolas Vacelet</i>	239
Bridging Refinement of Interface Automata to Forward Simulation of I/O Automata <i>Yanjun Wen, Ji Wang, Zhichang Qi</i>	259
Learning to Verify Safety Properties <i>Abhay Vardhan, Koushik Sen, Mahesh Viswanathan, Gul Agha</i>	274
Automatic Extraction of Object-Oriented Observer Abstractions from Unit-Test Executions <i>Tao Xie, David Notkin</i>	290

A Specification-Based Approach to Testing Polymorphic Attributes <i>Ling Liu, Huaikou Miao</i>	306
From <i>Circus</i> to JCSP <i>Marcel Oliveira, Ana Cavalcanti</i>	320
An Approach to Preserve Protocol Consistency and Executability Across Updates <i>Mahadevan Subramaniam, Parvathi Chundi</i>	341
A Formal Monitoring-Based Framework for Software Development and Analysis <i>Feng Chen, Marcelo D'Amorim, Grigore Roşu</i>	357
Verifying a File System Implementation <i>Konstantine Arkoudas, Karen Zee, Viktor Kuncak, Martin Rinard</i> ...	373
Verifying the On-line Help System of SIEMENS Magnetic Resonance Tomographs <i>Carsten Sinz, Wolfgang Küchlin</i>	391
Implementing Dynamic Aggregations of Abstract Machines in the B Method <i>Nazareno Aguirre, Juan Bicarregui, Lucio Guzmán, Tom Maibaum</i> ...	403
Formal Proof from UML Models <i>Nuno Amálio, Susan Stepney, Fiona Polack</i>	418
Interactive Verification of UML State Machines <i>Michael Balser, Simon Bäumlér, Alexander Knapp, Wolfgang Reif, Andreas Thums</i>	434
Refinement of Actions for Real-Time Concurrent Systems with Causal Ambiguity <i>Mila Majster-Cederbaum, Jinzhao Wu, Houguang Yue, Naijun Zhan</i> ..	449
From Durational Specifications to TLA Designs of Timed Automata <i>Yifeng Chen, Zhiming Liu</i>	464
Timed Patterns: TCOZ to Timed Automata <i>Jin Song Dong, Ping Hao, Sheng Chao Qin, Jun Sun, Wang Yi</i>	483
Author Index	499