

*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

*University of California, Los Angeles, CA, 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*

Zhiming Liu Jifeng He (Eds.)

# Formal Methods and Software Engineering

8th International Conference  
on Formal Engineering Methods, ICFEM 2006  
Macao, China, November 1-3, 2006  
Proceedings



Springer

Volume Editors

Zhiming Liu

The United Nations University  
International Institute for Software Technology  
UNU-IIS, Casa Silva Mendes Ext. do Engenheiro Trigo No. 4  
P.O. Box 3058, Macao SAR, China  
E-mail: z.liu@iist.unu.edu

Jifeng He

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

Library of Congress Control Number: 2006934465

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

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN            0302-9743  
ISBN-10        3-540-47460-9 Springer Berlin Heidelberg New York  
ISBN-13        978-3-540-47460-9 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

[springer.com](http://springer.com)

© Springer-Verlag Berlin Heidelberg 2006  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper    SPIN: 11901433    06/3142    5 4 3 2 1 0

# Preface

Formal methods for the development of computer systems have been extensively researched and studied. A range of semantic theories, specification languages, design techniques, and verification methods and tools have been developed and applied to the construction of programs of moderate size that are used in critical applications. The challenge now is to scale up formal methods and integrate them into engineering development processes for the correct construction and maintenance of computer systems. This requires us to improve the state of the art by researching the integration of methods and their theories, and merging them into industrial engineering practice, including new and emerging practice.

ICFEM, the *International Conference on Formal Engineering Methods*, 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. The conference particularly encourages research that aims at a combination of conceptual and methodological aspects with their formal foundation and tool support, and work that has been incorporated into the production of real systems.

This volume contains the proceedings of ICFEM 2006, which was the 8th ICFEM and held in Macao SAR, China on 1-3 November 2006. The Program Committee received 108 submissions from over 30 countries and regions. Each paper was reviewed, mostly by at least three referees working in relevant fields, but by two in a few cases. Borderline papers were further discussed during an online meeting of the Program Committee. A total of 38 papers were accepted based on originality, technical soundness, presentation and relevance to formal engineering and verification methods. We sincerely thank all the authors who submitted their work for consideration. We thank the Program Committee members and the other referees for their effort and professional work in the reviewing and selecting process. In addition to the regular papers, the proceedings also include contributions from the keynote speakers: Zhou Chaochen, Gary T. Leavens and John McDermid.

Three associated events were held: an Asian Working Conference on Verified Software (AWCVS06, 29-31 October), a Refinement Workshop (REFINE06, 31 October) and a Workshop on Formal Methods for Interactive Systems (FMIS06, 31 October). We thank the organizers for bringing their events to ICFEM 2006.

ICFEM 2006 was jointly organized and sponsored by the International Institute for Software Technology of the United Nations University (UNU-IIST), the University of Macau, and Macao Polytechnic Institute. We would like to thank all the members of staff and students who helped in the organization, in particular Pun Chong Iu, Pun Ka, Sandy Lee, Ho Sut Meng, Chan Iok Sam, Hoi Iok Wa, and Lu Yang. Acknowledgement also goes to Formal Method Europe for its support to the FME Keynote Speaker.

# Organization

## Conference Chairs

- Honorary Chair: Vai Pan Iu (Rector, University of Macau, Macao)  
Conference Chairs: Yiping Li (University of Macau, Macao)  
George Michael Reed (UNU-IIST, Macao)  
Program Chairs: He Jifeng (East China Normal University, China)  
Zhiming Liu (UNU-IIST, Macao)
- Organization Chairs: Iontong Iu (UNU-IIST, Macao)  
Xiaoshan Li (University of Macau, Macao)
- Publicity Chair: Chris George (UNU-IIST, Macao)  
Workshop Chair: Bernhard K. Aichernig (Graz Univ. of Tech., Austria)

## Program Committee

Farhad Arbab	Mathai Joseph	Peter H. Schmitt
Ralph Back	Kung-Kiu Lau	Klaus-Dieter Schewe
Luis Soares Barbosa	Xuandong Li	Wolfram Schulte
Tommaso Bolognesi	Tiziana Margaria	Joseph Sifakis
Jonathan P. Bowen	Hong Mei H	Joao Pedro Sousa
Manfred Broy	Huaikou Miao	Sofiene Tahar
Michael Butler	Ernst-Ruediger Olderog	T.H. Tse
Ana Cavalcanti	Shengchao Qin	Farn Wang
Yoonsik Cheon	Zongyan Qiu	Mark Utting
Philippe Darondeau	Anders P. Ravn	Martin Wirsing
Jim Davies	Ken Robinson	Qiwen Xu
Colin Fidge	Abhik Roychoudhury	Hongseok Yang
John Fitzgerald	Motoshi Saeki	Wang Yi
Marc Frappier	Hassen Saidi	Jian Zhang
Marcelo Frias	Augusto Sampaio	
Atsushi Igarashi	Davide Sangiorgi	

## External Referees

Poonam Agarwal	Leonid Kof	Katharina Spies
Frank Atanassow	Pavel Krcal	David Streader
Richard Banach	Marco Kuhrmann	Kim Solin
Pontus Boström	Vinay Kulkarni	Jun Sun
Judy Bowen	Shrawan Kumar	Bernhard Thalheim

Jeremy Bryans	Daan Leijen	Bernhard Schaetz
Michael Butler	Quan Long	Natalia Sidorova
Gustavo Cabral	Robi Malik	Colin Snook
Cristina Cershi-Seceleanu	Herve Marchand	Edward Turner
Jessica Chen	Joao Marques-Silva	Margus Veanes
Yiyun Chen	Leonid Mokrushin	R. Venkatesh
Tom Chothia	Mohammad Reza Mousavi	Phan Cong Vinh
Dave Clarke	Ravindra D. Naik	Hai Wang
Mehdi Dastani	Girish Keshav Palshikar	Shuling Wang
David Faitelson	Matthew Parkinson	Zheng Wang
Mauro Gaspari	Yu Pei	Ji Wang
Amjad Gawanmeh	Paul Pettersson	James Welch
Blaise Genest	Mike Poppleton	Harro Wimmel
Thomas Genet	Viorel Preoteasa	Divakar Yadav
Olga Grinchtein	Stephane Lo Presti	Hongli Yang
Ali Habibi	Rodrigo Ramos	Shaofa Yang
Tobias Hain	Nuno F. Rodrigues	Mohamed Zaki
Osman Hasan	Jan Romberg	Yan Zhang
Jounaidi Ben Hassen	Carlos Rubio	Jane Zhao
Roland Kaschek	Mehrnoosh Sadrzadeh	Jianhua Zhao
Stephanie Kemper	Amer Samara	Xiangpeng Zhao
Linas Laibinis	Thiago Santos	Sergiy Zlatkin
		Ping Zhu

### Steering Committee

Chair:	He Jifeng (East China Normal University, China)
Members:	Keijiro Araki (Kyushu University, Japan)
	Jin Song Dong (National University, Singapore)
	Chris George (UNU-IIST, Macao)
	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)

# Table of Contents

## Keynote Talks

Program Verification Through Computer Algebra . . . . .	1
<i>Chaochen Zhou</i>	
JML's Rich, Inherited Specifications for Behavioral Subtypes . . . . .	2
<i>Gary T. Leavens</i>	
Three Perspectives in Formal Engineering . . . . .	35
<i>John McDermid, Andy Galloway</i>	

## Specification and Verification

A Method for Formalizing, Analyzing, and Verifying Secure User Interfaces . . . . .	55
<i>Bernhard Beckert, Gerd Beuster</i>	
Applying Timed Interval Calculus to Simulink Diagrams . . . . .	74
<i>Chunqing Chen, Jin Song Dong</i>	
Reducing Model Checking of the Few to the One . . . . .	94
<i>E. Allen Emerson, Richard J. Trefler, Thomas Wahl</i>	
Induction-Guided Falsification . . . . .	114
<i>Kazuhiro Ogata, Masahiro Nakano, Weiqiang Kong, Kokichi Futatsugi</i>	
Verifying $\chi$ Models of Industrial Systems with SPIN . . . . .	132
<i>Nikola Trčka</i>	
Stateful Dynamic Partial-Order Reduction . . . . .	149
<i>Xiaodong Yi, Ji Wang, Xuejun Yang</i>	

## Internetware and Web-Based Systems

User-Defined Atomicity Constraint: A More Flexible Transaction Model for Reliable Service Composition . . . . .	168
<i>Xiaoning Ding, Jun Wei, Tao Huang</i>	

Environment Ontology-Based Capability Specification for Web  
Service Discovery ..... 185  
*Puwei Wang, Zhi Jin, Lin Liu*

Scenario-Based Component Behavior Derivation ..... 206  
*Yan Zhang, Jun Hu, Xiaofeng Yu, Tian Zhang,  
Xuandong Li, Guoliang Zheng*

Verification of Computation Orchestration Via Timed  
Automata ..... 226  
*Jin Song Dong, Yang Liu, Jun Sun, Xian Zhang*

Towards the Semantics for Web Service Choreography  
Description Language ..... 246  
*Jing Li, Jifeng He, Geguang Pu, Huibiao Zhu*

Type Checking Choreography Description Language ..... 264  
*Hongli Yang, Xiangpeng Zhao, Zongyan Qiu, Chao Cai,  
Geguang Pu*

**Concurrent, Communicating, Timing  
and Probabilistic Systems**

Formalising Progress Properties of Non-blocking Programs ..... 284  
*Brijesh Dongol*

Towards a Fully Generic Theory of Data ..... 304  
*Douglas A. Creager, Andrew C. Simpson*

Verifying Statechart Statecharts Using CSP and FDR ..... 324  
*A.W. Roscoe, Z. Wu*

A Reasoning Method for Timed CSP Based on Constraint  
Solving ..... 342  
*Jin Song Dong, Ping Hao, Jun Sun, Xian Zhang*

Mapping RT-LOTOS Specifications into Time Petri Nets ..... 360  
*Tarek Sadani, Marc Boyer, Pierre de Saqui-Sannes,  
Jean-Pierre Courtiat*

Reasoning Algebraically About Probabilistic Loops ..... 380  
*Larissa Meinicke, Ian J. Hayes*



## Object and Component Orientation

Formal Verification of the Heap Manager of an Operating System Using Separation Logic . . . . .	400
<i>Nicolas Marti, Reynald Affeldt, Akinori Yonezawa</i>	
A Statically Verifiable Programming Model for Concurrent Object-Oriented Programs . . . . .	420
<i>Bart Jacobs, Jan Smans, Frank Piessens, Wolfram Schulte</i>	
Model Checking Dynamic UML Consistency . . . . .	440
<i>Xiangpeng Zhao, Quan Long, Zongyan Qiu</i>	

## Testing and Model Checking

Conditions for Avoiding Controllability Problems in Distributed Testing . . . . .	460
<i>Jessica Chen, Lihua Duan</i>	
Generating Test Cases for Constraint Automata by Genetic Symbiosis Algorithm . . . . .	478
<i>Samira Tasharoft, Sepand Ansari, Marjan Sirjani</i>	
Checking the Conformance of Java Classes Against Algebraic Specifications . . . . .	494
<i>Isabel Nunes, Antónia Lopes, Vasco Vasconcelos, João Abreu, Luís S. Reis</i>	
Incremental Slicing . . . . .	514
<i>Heike Wehrheim</i>	
Assume-Guarantee Software Verification Based on Game Semantics . . . . .	529
<i>Aleksandar Dimovski, Ranko Lazić</i>	
Optimized Execution of Deterministic Blocks in Java PathFinder . . . . .	549
<i>Marcelo d'Amorim, Ahmed Sobeih, Darko Marinov</i>	

## Tools

A Tool for a Formal Pattern Modeling Language . . . . .	568
<i>Soon-Kyeong Kim, David Carrington</i>	

An Open Extensible Tool Environment for Event-B ..... 588  
*Jean-Raymond Abrial, Michael Butler, Stefan Hallerstede,  
 Laurent Voisin*

Tool for Translating Simulink Models into Input Language  
of a Model Checker ..... 606  
*Meenakshi B., Abhishek Bhatnagar, Sudeepa Roy*

**Fault-Tolerance and Security**

Verifying Abstract Information Flow Properties in Fault Tolerant  
Security Devices ..... 621  
*Tim McComb, Luke Wildman*

A Language for Modeling Network Availability ..... 639  
*Luigia Petre, Kaisa Sere, Marina Waldén*

Multi-process Systems Analysis Using Event B: Application to Group  
Communication Systems ..... 660  
*J. Christian Attiogbé*

**Specification and Refinement**

Issues in Implementing a Model Checker for Z ..... 678  
*John Derrick, Siobhán North, Tony Simons*

Taking Our Own Medicine: Applying the Refinement Calculus  
to State-Rich Refinement Model Checking ..... 697  
*Leo Freitas, Ana Cavalcanti, Jim Woodcock*

Discovering Likely Method Specifications ..... 717  
*Nikolai Tillmann, Feng Chen, Wolfram Schulte*

Time Aware Modelling and Analysis of Multiclocked VLSI Systems ..... 737  
*Tomi Westerlund, Juha Plosila*

SALT—Structured Assertion Language for Temporal Logic ..... 757  
*Andreas Bauer, Martin Leucker, Jonathan Streit*

**Author Index** ..... 777