Preface

This volume contains papers presented at the 7th International Conference on Formal Engineering Methods (ICFEM 2005), 1–4 November 2005, Manchester, UK.

Formal engineering methods are changing the way that systems are developed. With language and tool support, these methods are being used for semi-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 aim of ICFEM 2005 was to bring together those interested in the application of formal engineering methods to computer systems. Researchers and practitioners, from industry, academia, and government, were encouraged to attend, and to help advance the state of the art.

The conference was supported by sponsorships from Microsoft Research, USA, the Software Engineers Association of Japan, the University of Manchester, Manchester City Council, Formal Methods Europe (FME) and the British Computer Society Formal Aspects of Computing Specialist Group (BCS-FACS). We wish to thank these sponsors for their generosity.

The final programme consisted of 3 invited talks and 30 technical papers selected from a total of 74 submissions. The invited speakers were: Anthony Hall, independent consultant, UK; Egon Börger, University of Pisa, Italy; John Rushby, SRI, USA. Their talks were sponsored by BCS-FACS, Microsoft Research and FME respectively. We wish to thank the invited speakers for their inspiring talks.

Our heartfelt thanks go to all the members of the Programme Committee for their hard and conscientious work in reviewing and selecting the papers at various stages. I would also like to thank all the additional reviewers for their efforts and professionalism.

For organizing ICFEM 2005, we would like to thank the workshops and tutorials chair Mike Poppleton, the publicity chair Kenji Taguchi, the local organization chair Dave Lester, and the web-masters Elton Ballhysa and Faris Taweel. Their efforts were pivotal for the success of ICFEM 2005.

Finally, we would like to thank all the authors who submitted papers and all the conference attendees.

September 2005

Kung-Kiu Lau and Richard Banach
Manchester
Organization

Conference Chair

Richard Banach  University of Manchester, UK

Programme Chair

Kung-Kiu Lau  University of Manchester, UK

Programme Committee

Farhad Arbab  CWI and Leiden University, The Netherlands; University of Waterloo, Canada
Richard Banach  University of Manchester, UK
Luis Soares Barbosa  Minho University, Portugal
Mike Barnett  Microsoft Research, USA
Eerke Boiten  University of Kent, UK
Tommaso Bolognesi  CNR-ISTI, Italy
Marcello Bonsangue  Leiden University, The Netherlands
Jonathan P. Bowen  London South Bank University, UK
Manfred Broy  Technische Universität München, Germany
Bettina Buth  HAW Hamburg, Germany
Ana Cavalcanti  University of York, UK
Michel Charpentier  University of New Hampshire, USA
Jim Davies  University of Oxford, UK
Jin Song Dong  National University of Singapore, Singapore
Kai Engelhardt  University of New South Wales and NICTA, Australia
Colin Fidge  Queensland University of Technology, Australia
Mamoun Filali Amine  Université Paul Sabatier, France
John Fitzgerald  University of Newcastle upon Tyne, UK
Marc Frappier  Université de Sherbrooke, Canada
Dimitra Giannakopoulou  USRA/NASA Ames, USA
Chris George  United Nations University, China
Wolfgang Grieskamp  Microsoft Research, USA
Lindsay Groves  Victoria University of Wellington, New Zealand
Henri Habrias  Université de Nantes, France
Andrew Ireland  Heriot-Watt University, UK
Thomas Jensen  IRISA/CNRS, France
Soon-Kyeong Kim  University of Queensland, Australia
Steve King  University of York, UK
Rom Langerak  University of Twente, The Netherlands
James Larus  Microsoft Research, USA
Kung-Kiu Lau  University of Manchester, UK
### VIII Organization

<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark Lawford</td>
<td>McMaster University, Canada</td>
</tr>
<tr>
<td>Yves Ledru</td>
<td>LSR/IMAG, Domaine Universitaire, France</td>
</tr>
<tr>
<td>Peter A. Lindsay</td>
<td>University of Queensland, Australia</td>
</tr>
<tr>
<td>Shaoying Liu</td>
<td>Hosei University, Japan</td>
</tr>
<tr>
<td>Zhiming Liu</td>
<td>UNU-IIST, China</td>
</tr>
<tr>
<td>Brendan Mahony</td>
<td>Defence Science and Technology Organisation, Australia</td>
</tr>
<tr>
<td>Tiziana Margaria</td>
<td>University of Göttingen, Germany</td>
</tr>
<tr>
<td>Brad Martin</td>
<td>US Department of Defense, USA</td>
</tr>
<tr>
<td>Dominique Mery</td>
<td>Université Henri Poincaré Nancy 1, France</td>
</tr>
<tr>
<td>Huaikou Miao</td>
<td>Shanghai University, China</td>
</tr>
<tr>
<td>Alexandre Mota</td>
<td>Federal University of Pernambuco, Brazil</td>
</tr>
<tr>
<td>David Naumann</td>
<td>Stevens Institute of Technology, USA</td>
</tr>
<tr>
<td>Richard Paige</td>
<td>University of York, UK</td>
</tr>
<tr>
<td>Iman Poernomo</td>
<td>King's College London, UK</td>
</tr>
<tr>
<td>Fiona Polack</td>
<td>University of York, UK</td>
</tr>
<tr>
<td>Michael Poppleton</td>
<td>University of Southampton, UK</td>
</tr>
<tr>
<td>Steve Reeves</td>
<td>University of Waikato, New Zealand</td>
</tr>
<tr>
<td>Ken Robinson</td>
<td>University of New South Wales, Australia</td>
</tr>
<tr>
<td>Abhik Roychoudhury</td>
<td>National University of Singapore, Singapore</td>
</tr>
<tr>
<td>Harald Ruess</td>
<td>SRI International, USA</td>
</tr>
<tr>
<td>Motoshi Saeki</td>
<td>Tokyo Institute of Technology, Japan</td>
</tr>
<tr>
<td>Thomas Santen</td>
<td>Technische Universität Berlin, Germany</td>
</tr>
<tr>
<td>Klaus-Dieter Schewe</td>
<td>Massey University, New Zealand</td>
</tr>
<tr>
<td>Wolfram Schulte</td>
<td>Microsoft Research, USA</td>
</tr>
<tr>
<td>Kaisa Sere</td>
<td>Åbo Akademi University, Finland</td>
</tr>
<tr>
<td>Paul Strooper</td>
<td>University of Queensland, Australia</td>
</tr>
<tr>
<td>Asuman Suenbuel</td>
<td>SAP Research, USA</td>
</tr>
<tr>
<td>Paul A. Swatman</td>
<td>University of South Australia, Australia</td>
</tr>
<tr>
<td>Kenji Taguchi</td>
<td>National Institute of Informatics, Tokyo, Japan</td>
</tr>
<tr>
<td>Sofiene Tahar</td>
<td>Concordia University, Canada</td>
</tr>
<tr>
<td>Tetsuo Tamai</td>
<td>University of Tokyo, Japan</td>
</tr>
<tr>
<td>T.H. Tse</td>
<td>University of Hong Kong, China</td>
</tr>
<tr>
<td>Margus Veanes</td>
<td>Microsoft Research, USA</td>
</tr>
<tr>
<td>Charles Wallace</td>
<td>Michigan Technological University, USA</td>
</tr>
<tr>
<td>Farn Wang</td>
<td>National Taiwan University, Taiwan</td>
</tr>
<tr>
<td>Wang Yi</td>
<td>Uppsala University, Sweden</td>
</tr>
<tr>
<td>Jim Woodcock</td>
<td>University of York, UK</td>
</tr>
</tbody>
</table>

### Additional Referees

<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pascal André</td>
<td>Jean-Paul Bodeveix</td>
</tr>
<tr>
<td>Marcelo Arenas</td>
<td>Jeremy Bryans</td>
</tr>
<tr>
<td>Christian Attiogbé</td>
<td>Michael Butler</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Yuzhang Feng  
David Faitelson  
Benoit Fraikin  
Amjad Gawanmeh  
Frédéric Gervais  
Irina Mariuca  
Gheorghita  
Ben Gorry  
Jens Grabowski  
Olga Grinchtein  
Juan Guillen-Scholten  
Neil Henderson  
Lutz Kettner  
Bas Luttik  
Tom Maibaum  
Frank Marschall  
Tim McComb  
Sun Meng  
Haja Moinudeen  
Shin Nakamima  
O. Nasr  
Lemai Nguyen  
Corina Pasareanu  
Pascal Poizat  
M. Rached  
Rodrigo Ramos  
Pritam Roy  
Johann Schumann  
Emil Sekerinski  
Qin Shengchao  
Rakesh Shukla  
Colin Snook  
Maria Sorea  
Graham Steel  
Bernhard Steffen  
Jing Sun  
Willem Visser  
Nabil Wageeh  
Marina Waldén  
Geoffrey Watson  
James Welch  
Mohamed Zaki  
Sergiy Zlatkin
# Table of Contents

## Invited Talks

Realising the Benefits of Formal Methods
  *Anthony Hall* .................................................. 1

A Compositional Framework for Service Interaction Patterns and Interaction Flows
  *Alistair Barros, Egon Börger* ................................. 5

An Evidential Tool Bus
  *John Rushby* ..................................................... 36

## Specification

Derivation of UML Class Diagrams as Static Views of Formal B Developments
  *Akram Idani, Yves Ledru, Didier Bert* .......................... 37

29 New Unclarities in the Semantics of UML 2.0 State Machines
  *Harald Fecher, Jens Schönborn, Marcel Kyas, Willem-Paul de Roever* ............................. 52

The Semantics and Tool Support of OZTA
  *Jin Song Dong, Ping Hao, Shengchao Qin, Xian Zhang* ............. 66

## Modelling

An Abstract Model for Process Mediation
  *Michael Altenhofen, Egon Börger, Jens Lemcke* .................. 81

How Symbolic Animation Can Help Designing an Efficient Formal Model
  *Fabrice Bouquet, Frédéric Dadeau, Bruno Legeard* ................ 96

## Security

A Theory of Secure Control Flow
  *Martín Abadi, Mihai Budiu, Úlfar Erlingsson, Jay Ligatti* ........ 111

Game Semantics Model for Security Protocols
  *Mourad Debbabi, Mohamed Saleh* ................................. 125
Communication

Towards Dynamically Communicating Abstract Machines in the B Method
  Nazareno Aguirre, Marcelo Arroyo, Juan Bicarregui, Lucio Guzmán, Tom Maibaum .................................................. 141

Sweep-Line Analysis of TCP Connection Management
  Guy Edward Gallasch, Bing Han, Jonathan Billington ................. 156

2/3 Alternating Simulation Between Interface Automata
  Yanjun Wen, Ji Wang, Zhichang Qi ........................................ 173

Development

Formal Model-Driven Development of Communicating Systems
  Linas Laibinis, Elena Troubitsyna, Sari Leppänen, Johan Lilius,
  Qaisar Malik ................................................................. 188

JAHUEL: A Formal Framework for Software Synthesis
  I. Assayad, V. Bertin, F.-X. Defaut, Ph. Gerner, O. Quévrefeu,
  S. Yovine ................................................................. 204

Modelling and Refinement of an On-Chip Communication Architecture
  Juha Plosila, Pasi Liljeberg, Jouni Isoaho ............................... 219

Testing

  Ahmed Sobeih, Mahesh Viswanathan, Darko Marinov,
  Jennifer C. Hou ............................................................. 235

Adaptive Random Testing by Bisection with Restriction
  Johannes Mayer ............................................................... 251

Testing Real-Time Multi Input-Output Systems
  Laura Brandán Briones, Ed Brinksma .................................. 264

Verification

Formal Verification of a Memory Model for C-Like Imperative Languages
  Sandrine Blazy, Xavier Leroy ................................................ 280
Symbolic Verification of Distributed Real-Time Systems with Complex Synchronizations
Farn Wang ................................................... 300

An Improved Rule for While Loops in Deductive Program Verification
Bernhard Beckert, Steffen Schlager, Peter H. Schmitt ................. 315

Using Stålmarck’s Algorithm to Prove Inequalities
Byron Cook, Georges Gonthier ........................................... 330

Automatic Refinement Checking for B
Michael Leuschel, Michael Butler ....................................... 345

Slicing an Integrated Formal Method for Verification
Ingo Brückner, Heike Wehrheim ......................................... 360

A Static Communication Elimination Algorithm for Distributed System Verification
Francesc Babot, Miquel Bertran, August Climent ......................... 375

Incremental Verification of Owicki/Gries Proof Outlines Using PVS
Arjan J. Mooij, Wieger Wesselink .................................... 390

Using Three-Valued Logic to Specify and Verify Algorithms of Computational Geometry
Jens Brandt, Klaus Schneider ........................................... 405

Tools

An Automated Approach to Specification-Based Program Inspection
Shaoying Liu, Fumiko Nagoya, Yuting Chen, Masashi Goya,
John A. McDermid .................................................. 421

Visualizing and Simulating Semantic Web Services Ontologies
Jun Sun, Yuan Fang Li, Hai Wang, Jing Sun ......................... 435

A Model-to-Implementation Mapping Tool for Automated Model-Based GUI Testing
Ana C.R. Paiva, João C.P. Faria, Nikolai Tillmann,
Raul A.M. Vidal .................................................. 450

ClawZ: Cost-Effective Formal Verification for Control Systems
M.M. Adams, P.B. Clayton ........................................... 465