

Preface

The design and analysis of computing systems presents a significant challenge: systems need to be understood at many different levels of abstraction, and examined from many different perspectives. Formal methods—languages, tools, and techniques with a sound, mathematical basis—can be used to develop a thorough understanding, and to support rigorous examination.

Further research into effective integration is required if these methods are to have a significant impact outside academia. The Integrated Formal Methods (IFM) series of conferences seeks to promote that research, to bring together the researchers carrying it out, and to disseminate the results of that research among the wider academic and industrial community.

Earlier meetings in the series were held at: York (1999); Dagstuhl (2000); Turku (2002); Kent (2004); Eindhoven (2005). IFM 2007 is the largest to date, with 32 technical papers (from 85 submissions), 3 invited talks, 3 workshops, and a tutorial. The success of the series reflects the enthusiasm and efforts of the IFM community, and the organisers would like to thank the speakers, the committee, and the reviewers for their contributions.

Jim Davies and Jeremy Gibbons
Oxford, April 2007

Organisation

Chair

Jim Davies

Co-chairs

Jin Song Dong, Jeremy Gibbons, Judi Romijn, Wolfram Schulte

Workshops and Tutorials

Richard Paige

Local Arrangements

Jackie Jordan, James Welch

Special Sessions

Yifeng Chen, Eerke Boiten, Phil Brooke, John Derrick, Graeme Smith

Programme Committee

Didier Bert, Eerke Boiten, Jonathan Bowen, Phil Brooke, Michael Butler, Yifeng Chen, Paul Curzon, Jim Davies, John Derrick, Jin Song Dong, Steve Dunne, Andy Galloway, Chris George, Jeremy Gibbons, Wolfgang Grieskamp, Henri Habrias, Maritta Heisel, Soon-Kyeong Kim, Michel Lemoine, Shaoying Liu, Dominique Mery, Stephan Merz, Colin O'Halloran, Richard Paige, Luigia Petre, Jaco van de Pol, Judi Romijn, Thomas Santen, Steve Schneider, Wolfram Schulte, Kaisa Sere, Jane Sinclair, Graeme Smith, Bill Stoddart, Kenji Taguchi, Helen Treharne, Heike Wehrheim, Kirsten Winter, Jim Woodcock

Additional reviewers

Pascal Andre, Christian Attiogbé, Pavel Avgustinov, Luis Barbosa, Alessandra Cavarra, Orieta Celiku, Yuting Chen, Chunqing Chen, John Colley, Robert Colvin, Neil Evans, Yuan Fang Li, Berndt Farwer, Diego Garbervetsky, Lars Grunske, Stefan Hallerstedde, Dubravka Ilic, Yoshinao Isobe, Jon Jacky, Ehtesham Jam, Linas Laibinis, Antonia Lopes, Eduardo Lopez-Ruiz, Hidehiko Masuhara, Tim McComb, Larissa Meinicke, Bernhard Moeller, Leonardo de Moura, Ivan Porres, Viorel Preoteasa, Franco Raimondi, Jean-Luc Richier, Rimvydas Ruksenas, Ondrej Rypacek, Holger Schmidt, Cristina Seceleanu, Paul Strooper, Georg Struth, Jun Sun, Jörn Guy Süß, Yoshinori Tanabe, Nikolai Tillmann, Jan Tobias Muehlberg, Niki Trigoni, Margus Veanes, Meng Wang, Geoffrey Watson, James Welch, Luke Wildman, Divakar Yadav, Lu Yan, Huibiao Zhu

Table of Contents

Verifying Temporal Properties of CommUnity Designs	1
<i>Nazareno Aguirre, Germán Regis, and Tom Maibaum</i>	
Precise Scenarios – A Customer-Friendly Foundation for Formal Specifications	21
<i>Oliver Au, Roger Stone, and John Cooke</i>	
Automated Verification of Security Policies in Mobile Code	37
<i>Chiara Braghin, Natasha Sharygina, and Katerina Barone-Adesi</i>	
Slicing Concurrent Real-Time System Specifications for Verification	54
<i>Ingo Brückner</i>	
Slotted-Circus: A UTP-Family of Reactive Theories	74
<i>Andrew Butterfield, Adnan Sherif, and Jim Woodcock</i>	
Bug Hunting with False Negatives	98
<i>Jens Calamé, Natalia Ioustinova, Jaco van de Pol, and Natalia Sidorova</i>	
Behavioural Specifications from Class Models	118
<i>Alessandra Cavarra and James Welch</i>	
Inheriting Laws for Processes with States	138
<i>Yifeng Chen</i>	
Probabilistic Timed Behavior Trees	156
<i>Robert Colvin, Lars Grunske, and Kirsten Winter</i>	
Guiding the Correction of Parameterized Specifications	176
<i>Jean-François Couchot and Frédéric Dadeau</i>	
Proving linearizability via non-atomic refinement	196
<i>John Derrick, Gerhard Schellhorn, and Heike Wehrheim</i>	
Lifting General Correctness into Partial Correctness is <i>ok</i>	216
<i>Steve Dunne and Andy Galloway</i>	
Verifying CSP-OZ-DC Specifications with Complex Data Types and Timing Parameters	234
<i>Johannes Faber, Swen Jacobs, and Viorica Sofronie-Stokkermans</i>	
Modelling and Verification of the LMAC Protocol for Wireless Sensor Networks	254
<i>Ansgar Fehnker, Lodewijk van Hoesel, Angelika Mader</i>	

VIII

Finding State Solutions to Temporal Logic Queries	274
<i>Mihaela Gheorghiu, Arie Gurfinkel, and Marsha Chechik</i>	
Qualitative Probabilistic Modelling in Event-B	294
<i>Stefan Hallerstede and Thai Son Hoang</i>	
Verifying Smart Card Applications: An ASM Approach	314
<i>Dominik Haneberg, Holger Grandy, Wolfgang Reif, and Gerhard Schellhorn</i>	
Verification of Probabilistic Properties in HOL using the Cumulative Distribution Function	334
<i>Osman Hasan and Sofiène Tahar</i>	
UTP Semantics for Web Services	354
<i>He Jifeng</i>	
Combining Mobility With State	374
<i>Damien Karkinsky, Steve Schneider, and Helen Treharne</i>	
Algebraic Approaches to Formal Analysis of the Mondex Electronic Purse System	394
<i>Weiqiang Kong, Kazuhiro Ogata, and Kokichi Futatsugi</i>	
Capturing Conflict and Confusion in CSP	414
<i>Christie Marr (née Bolton)</i>	
A Stepwise Development Process for Reasoning about the Reliability of Real-time Systems	435
<i>Larissa Meinicke and Graeme Smith</i>	
Decomposing Integrated Specifications for Verification	455
<i>Björn Metzler</i>	
Validating Z Specifications using the PROB Animator and Model Checker	475
<i>Daniel Plagge and Michael Leuschel</i>	
Verification of multi-agent negotiations using the Alloy Analyzer	495
<i>Rodion Podorozhny, Sarfraz Khurshid, Dewayne Perry, and Xiaoqin Zhang</i>	
Integrated Static Analysis for Linux Device Driver Verification	513
<i>Hendrik Post and Wolfgang Kuchlin</i>	
Integrating verification, testing, and learning for cryptographic protocols	533
<i>Martijn Oostdijk, Vlad Rusu, Jan Tretmans, Rene de Vries, and Tim Willemse</i>	
Translating FSP into LOTOS and Networks of Automata	553
<i>Gwen Salaün, Jeff Kramer, Frédéric Lang, and Jeff Magee</i>	

Common Semantics for Use Cases and Task Models	574
<i>Daniel Sinnig, Patrice Chalin, and Ferhat Khendek</i>	
Unifying Theories of Objects	594
<i>Michael Anthony Smith and Jeremy Gibbons</i>	
Non-Interference Properties for Data-Type Reduction of Communicating Systems	614
<i>Tobe Toben</i>	
Co-simulation of Distributed Embedded Real-Time Control Systems	634
<i>Marcel Verhoef, Peter Visser, Jozef Hooman, and Jan Broenink</i>	
Author Index	654