

Lecture Notes in Computer Science

2999

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer

Berlin

Heidelberg

New York

Hong Kong

London

Milan

Paris

Tokyo

Eerke A. Boiten John Derrick
Graeme Smith (Eds.)

Integrated Formal Methods

4th International Conference, IFM 2004
Canterbury, UK, April 4-7, 2004
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Eerke A. Boiten
John Derrick
University of Kent
Computing Laboratory
Canterbury, Kent, CT2 7NF, UK
E-mail: {E.A.Boiten/J.Derrick}@kent.ac.uk
Graeme Smith
University of Queensland
School of Information Technology and Electrical Engineering
4072 Brisbane, Australia
E-mail: smith@itee.uq.edu.au

Library of Congress Control Number: 2004102974

CR Subject Classification (1998): F.3, D.3, D.2, D.1

ISSN 0302-9743

ISBN 3-540-21377-5 Springer-Verlag 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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag 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 PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 10992623 06/3142 5 4 3 2 1 0

Preface

The fourth conference in the series of international meetings on Integrated Formal Methods, IFM, was held in Canterbury, UK, 4–7 April 2004. The conference was organized by the Computing Laboratory at the University of Kent, whose main campus is just outside the ancient town of Canterbury, part of the county of Kent.

Kent is situated in the southeast of England, and the university sits on a hill overlooking the city of Canterbury and its world-renowned cathedral. The University of Kent was granted its Royal Charter in 1965. Today there are almost 10,000 full-time and part-time students, with over 110 nationalities represented.

The IFM meetings have proven to be particularly successful. The first meeting was held in York in 1999, and subsequently we held events in Germany in 2000, and then Finland in 2002. The conferences are held every 18 months or so, and attract a wide range of participants from Europe, the Americas, Asia and Australia. The conference is now firmly part of the formal methods conference calendar. The conference has also evolved in terms of themes and subjects represented, and this year, in line with the subject as a whole, we saw more work on verification as some of the challenges in this subject are being met.

The work reported at IFM conferences can be seen as part of the attempt to manage complexity by combining paradigms of specification and design, so that the most appropriate design tools are used at different points in the life-cycle. In part this is about combining specification formalisms, and this happens, for example, when one combines state-based and event-based languages to produce integrated notations capable of covering a wider range of the design spectrum than would otherwise be feasible. However, the work of IFM goes beyond that, as we can see in this proceedings.

Indeed, increasingly specification is only the start of a process that includes verification as an explicit aim, and this work was heavily represented in this year's conference. This was also reflected in the talks by invited speakers who represented both academic and industry perspectives on the subject.

Tom Ball talked about his team's work on SLAM and the static driver verifier, and described the use of formal methods in Microsoft. Ursula Martin, of Queen Mary, University of London, talked about her work on design verification for control engineering, and Tom Melham of Oxford gave a talk entitled "Integrating Model Checking and Theorem Proving in a Reflective Functional Language." Tom Ball's talk was sponsored by FME (Formal Methods Europe), to whom we are particularly grateful. FME also held their Annual General Meeting on the Sunday prior to the main conference. We are also grateful to Jim Woodcock for agreeing to give a tutorial on the Unifying Theories of Programming, jointly with Ana Cavalcanti. FORTEST, a UK national network on Formal Methods and Testing, also joined us for the final day when members attended talks on testing and then held an informal workshop after the main conference.

The contributed talks were grouped into a number of sessions, this year covering:

- Automating program analysis
- State-/event-based verification
- Formalizing graphical notations
- Refinement
- Object orientation
- Hybrid and timed automata
- Integration frameworks
- Verifying interactive systems
- Testing and assertions

In total there were 65 submissions, of which we accepted 24 after the usual refereeing process. We are grateful to all those involved in the reviewing process and subsequent programme committee discussion. An important note of thanks must also be given to all those who helped locally.

We hope that these proceedings will serve as a useful source of reference for not only the attendees, but also the wider community. We look forward to further IFM meetings where we can continue the discussion on the best ways to engineer both hardware and software systems with the ultimate aim of increased reliability and robustness.

April 2004

Eerke Boiten
John Derrick
Graeme Smith

Program Committee

Didier Bert (France)	Susumu Hayashi (Japan)
Eerke Boiten (Co-chair, UK)	Maritta Heisel (Germany)
Jonathan Bowen (UK)	Michel Lemoine (France)
Michael Butler (UK)	Shaoying Liu (Japan)
Paul Curzon (UK)	Dominique Méry (France)
Jim Davies (UK)	Luigia Petre (Finland)
John Derrick (Co-chair, UK)	Judi Romijn (The Netherlands)
Jin Song Dong (Singapore)	Thomas Santen (Germany)
John Fitzgerald (UK)	Steve Schneider (UK)
Andrew Galloway (UK)	Wolfram Schulte (US)
Chris George (Macau)	Kaisa Sere (Finland)
Wolfgang Grieskamp (US)	Jane Sinclair (UK)
Henri Habrias (France)	Graeme Smith (Co-chair, Australia)

Bill Stoddart (UK)
 Kenji Taguchi (UK)
 W.J. (Hans) Toetenel
 (The Netherlands)

Heike Wehrheim (Germany)
 Kirsten Winter (Australia)
 Jim Woodcock (UK)

Sponsors

In addition to FME sponsorship of an invited talk, we are grateful to BCS FACS (the Formal Aspects of Computing Science Specialist Group of the British Computer Society, <http://www.bcs.org.uk/>) for sponsoring the best paper award.



External Referees

All submitted papers were reviewed by members of the program committee and a number of external referees, who produced extensive review reports and without whose work the conference would lose its quality status. To the best of our knowledge the list below is accurate. We apologize for any omissions or inaccuracies.

Bernhard K. Aichernig
 Marcus Alanen
 Pascal André
 Jim Armstrong
 Mike Barnett
 Gerd Behrmann
 Dag Björklund
 Victor Bos
 Pontus Boström
 Sylvain Boulmé
 Robert Büssow
 Ana Cavalcanti
 Orieta Celiku
 Christine Choppy
 Corina Cirstea
 Dang Van Hung
 Henning Dierks
 Roger Duke
 Steve Dunne
 Neil Evans
 Li Yuan Fang
 Ansgar Fehnker
 Leonardo Freitas

Biniam Gebremichael
 Michael Goldsmith
 Andy Gravell
 Stefan Hallerstede
 Ian Hayes
 Steffen Helke
 Jon Jacky
 Nigel Jefferson
 Sara Kalvala
 Maciej Koutny
 Yves Ledru
 Hui Liang
 Zhiming Liu
 Stephan Merz
 Pierre Michel
 Arjan J. Mooij
 MohammadReza
 Mousavi
 Catherine Oriat
 Stephen Paynter
 Maria
 Pietkiewicz-Koutny
 Juha Plosila

Pascal Poizat
 Mike Poppleton
 Ivan Porres
 Marie-Laure Potet
 Viorel Preoteasa
 Arend Rensink
 Steve Riddle
 Michael Rusinowitch
 Gwen Salaün
 Cristina Secleanu
 Dirk Seifert
 Colin Snook
 Mariëlle Stoelinga
 Cedric Stoquer
 Carsten Sühl
 Jun Sun
 Xinbei Tang
 Nikolai Tillmann
 Helen Treharne
 Leonidas Tsiopoulos
 Margus Veanes
 Sergiy Vilkomir
 Marina Waldén

Hai Wang
Virginie Wiels
Hirokazu Yatsu

Volker Zerbe
Frank Zeyda
Andrea Zisman

Steffen Zschaler

Table of Contents

Invited Talks

SLAM and Static Driver Verifier: Technology Transfer of Formal Methods inside Microsoft	1
<i>Thomas Ball, Byron Cook, Vladimir Levin, Sriram K. Rajamani</i>	
Design Verification for Control Engineering.....	21
<i>Richard J. Boulton, Hanne Gottliebse, Ruth Hardy, Tom Kelsey, Ursula Martin</i>	
Integrating Model Checking and Theorem Proving in a Reflective Functional Language	36
<i>Tom Melham</i>	

Tutorial

A Tutorial Introduction to Designs in Unifying Theories of Programming.....	40
<i>Jim Woodcock, Ana Cavalcanti</i>	

Contributed Papers

An Integration of Program Analysis and Automated Theorem Proving	67
<i>Bill J. Ellis, Andrew Ireland</i>	
Verifying Controlled Components	87
<i>Steve Schneider, Helen Treharne</i>	
Efficient CSP _Z Data Abstraction.....	108
<i>Adalberto Farias, Alexandre Mota, Augusto Sampaio</i>	
State/Event-Based Software Model Checking	128
<i>Sagar Chaki, Edmund M. Clarke, Joël Ouaknine, Natasha Sharygina, Nishant Sinha</i>	
Formalising Behaviour Trees with CSP	148
<i>Kirsten Winter</i>	
Generating MSCs from an Integrated Formal Specification Language	168
<i>Jin Song Dong, Shengchao Qin, Jun Sun</i>	

UML to B: Formal Verification of Object-Oriented Models	187
<i>K. Lano, D. Clark, K. Androutsopoulos</i>	
Software Verification with Integrated Data Type Refinement for Integer Arithmetic	207
<i>Bernhard Beckert, Steffen Schlager</i>	
Constituent Elements of a Correctness-Preserving UML Design Approach	227
<i>Tiberiu Seceleanu, Juha Plosila</i>	
Relating Data Independent Trace Checks in CSP with UNITY Reachability under a Normality Assumption	247
<i>Xu Wang, A.W. Roscoe, R.S. Lazić</i>	
Linking CSP-OZ with UML and Java: A Case Study	267
<i>Michael Möller, Ernst-Rüdiger Olderog, Holger Rasch, Heike Wehrheim</i>	
Object-Oriented Modelling with High-Level Modular Petri Nets.....	287
<i>Cécile Bui Thanh, Hanna Klaudel</i>	
Specification and Verification of Synchronizing Concurrent Objects	307
<i>Gabriel Ciobanu, Dorel Lucanu</i>	
Understanding Object-Z Operations as Generalised Substitutions	328
<i>Steve Dunne</i>	
Embeddings of Hybrid Automata in Process Algebra	343
<i>Tim A.C. Willemse</i>	
An Optimal Approach to Hardware/Software Partitioning for Synchronous Model	363
<i>Pu Geguang, Dang Van Hung, He Jifeng, Wang Yi</i>	
A Many-Valued Logic with Imperative Semantics for Incremental Specification of Timed Models	382
<i>Ana Fernández Vilas, José J. Pazos Arias, Rebeca P. Díaz Redondo, Alberto Gil Solla, Jorge García Duque</i>	
Integrating Temporal Logics	402
<i>Yifeng Chen, Zhiming Liu</i>	
Integration of Specification Languages Using Viewpoints	421
<i>Marius C. Bujorianu</i>	
Integrating Formal Methods by Unifying Abstractions	441
<i>Raymond Boute</i>	

Formally Justifying User-Centred Design Rules: A Case Study on Post-completion Errors	461
<i>Paul Curzon, Ann Blandford</i>	
Using UML Sequence Diagrams as the Basis for a Formal Test Description Language	481
<i>Simon Pickin, Jean-Marc Jézéquel</i>	
Viewpoint-Based Testing of Concurrent Components	501
<i>Luke Wildman, Roger Duke, Paul Strooper</i>	
A Method for Compiling and Executing Expressive Assertions	521
<i>F.J. Galán Morillo, J.M. Cañete Valdeón</i>	
Author Index	541