

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

John Fitzgerald Ian J. Hayes
Andrzej Tarlecki (Eds.)

FM 2005: Formal Methods

International Symposium of Formal Methods Europe
Newcastle, UK, July 18-22, 2005
Proceedings



Springer

Volume Editors

John Fitzgerald
University of Newcastle upon Tyne
Centre for Software Reliability
Newcastle upon Tyne, NE1 7RU, UK
E-mail: john.fitzgerald@ncl.ac.uk

Ian J. Hayes
University of Queensland
School of Information Technology and Electrical Engineering
Brisbane, QLD 4072, Australia
E-mail: Ian.Hayes@itee.uq.edu.au

Andrzej Tarlecki
Warsaw University
Faculty of Mathematics, Informatics and Mechanics
Banacha 2, 02-097 Warszawa, Poland
E-mail: tarlecki@mimuw.edu.pl

Library of Congress Control Number: 2005928720

CR Subject Classification (1998): D.2, F.3, D.3, D.1, J.1, K.6, F.4

ISSN	0302-9743
ISBN-10	3-540-27882-6 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-27882-5 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 2005
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11526841 06/3142 5 4 3 2 1 0

Preface

This volume contains the proceedings of Formal Methods 2005, the 13th International Symposium on Formal Methods held in Newcastle upon Tyne, UK, during July 18–22, 2005. Formal Methods Europe (FME, www.fmeurope.org) is an independent association which aims to stimulate the use of, and research on, formal methods for system development. FME conferences began with a VDM Europe symposium in 1987. Since then, the meetings have grown and have been held about once every 18 months. Throughout the years the symposia have been notably successful in bringing together researchers, tool developers, vendors, and users, both from academia and from industry. Formal Methods 2005 confirms this success.

We received 130 submissions to the main conference, from all over the world. Each submission was carefully refereed by at least three reviewers. Then, after an intensive, in-depth discussion, the Program Committee selected 31 papers for presentation at the conference. They form the bulk of this volume. We would like to thank all the Program Committee members and the referees for their excellent and efficient work.

Apart from the selected contributions, the Committee invited three keynote lectures from Mathai Joseph, Marie-Claude Gaudel and Chris Johnson. You will find the abstracts/papers for their keynote lectures in this volume as well.

An innovation for the FM 2005 program was a panel discussion on the history of formal methods, with Jean-Raymond Abrial, Dines Bjørner, Jim Horning and Cliff Jones as panelists. Unfortunately, it was not possible to reflect this event in the current volume, but you will find the material documenting it elsewhere (see the conference Web page).

An Industry Day was organized by the Formal Techniques Industrial Association (ForTIA) alongside the main symposium. This was directly related to the main theme of the FM symposia: the use of well-founded formal methods in the industrial practice of software design, development and maintenance. We have therefore included abstracts of the invited presentations in this volume as well.

The main FM 2005 conference was accompanied by 9 workshops and 11 tutorials.

The electronic submission, refereeing and Program Committee discussions would not have been possible without software support. We worked with the OCS system developed at the University of Dortmund — our thanks to the staff there for their support.

Finally, we would like to thank all those who helped to create and run the symposium in Newcastle, and in particular Claire Smith, Jon Warwick, Joan Atkinson, Sarah Davidson, Nigel Jefferson, Joey Coleman, Jeremy Bryans, Neil Henderson and Juan Bicarregui for their help in bringing the program, and these proceedings, together.

Organization

FM 2005 was organized by the Centre for Software Reliability at the University of Newcastle upon Tyne (www.csr.ncl.ac.uk) and Formal Methods Europe. We are grateful for the support of the University of Newcastle and its School of Computing Science. Within Formal Methods Europe, we are particularly grateful to Kees Pronk and Stefania Gnesi for their help with budgeting and organization. We also gladly acknowledge direct sponsorship from SAP Research and the British Computer Society Specialist Group on Formal Aspects of Computing Science (BCS-FACS).

Conference Chairs

General Chair	John S. Fitzgerald, University of Newcastle, UK
Program Co-chairs	Ian Hayes, University of Queensland, Australia Andrzej Tarlecki, Warsaw University, Poland
Conference Organizer	Claire Smith, University of Newcastle, UK
Finance Chair	Jon Warwick, University of Newcastle, UK
Tools Exhibition Chair	Joan Atkinson, University of Newcastle, UK
Workshops Chair	Juan Bicarregui, Rutherford Appleton Laboratory, UK
Tutorials Chair	Neil Henderson, University of Newcastle, UK

Program Committee

Bernhard Aichernig, UNU-IIST, Macau, China
Keijiro Araki, Kyushu University, Japan
Juan Bicarregui, Rutherford Appleton Laboratory, UK
Michel Bidoit, LSV, CNRS and ENS de Cachan, France
Ed Brinksma, University of Twente, The Netherlands
Luca Cardelli, Microsoft Research, UK
Ernie Cohen, Microsoft, USA
Jin Song Dong, National University of Singapore, Singapore
José Luiz Fiadeiro, University of Leicester, UK
John S. Fitzgerald, Centre for Software Reliability, UK
Stefania Gnesi, CNR, Italy
Anthony Hall, UK
Anne E. Haxthausen, Technical University of Denmark, Denmark
Ian Hayes, University of Queensland, Australia (Co-chair)
Thomas A. Henzinger, EPFL and University of California, Berkeley, USA
He Jifeng, UNU-IIST, Macau, China
Cliff Jones, University of Newcastle, UK

Shaoying Liu, Hosei University, Japan
 Mícheál Mac an Aírchinnigh, Trinity College Dublin, Ireland
 Tom Maibaum, McMaster University, Canada
 Dino Mandrioli, Politecnico di Milano, Italy
 Tobias Nipkow, Technische Universität München, Germany
 José Oliveira, Universidade do Minho, Portugal
 Sam Owre, CRI, USA
 Alexander Petrenko, ISPRAS, Russia
 Nico Plat, West Consulting, The Netherlands
 Ken Robinson, University of New South Wales, Australia
 Mark Saaltink, ORA Canada, Canada
 Shin Sahara, JFITS, Japan
 Steve Schneider, University of Surrey, UK
 Kaisa Sere, Åbo Akademi, Finland
 Ketil Stølen, SINTEF, Norway
 Andrzej Tarlecki, Warsaw University, Poland (Co-chair)
 Mark Utting, Waikato University, New Zealand
 Marcel Verhoef, Chess IT and Radboud University, Nijmegen, Netherlands
 Alan Wassing, McMaster University, Canada
 Martin Wirsing, Ludwig-Maximilians-Universität, München, Germany

Referees

Carlos Bacelar Almeida	Gyrd Brændeland	Martin Fränzle
Paulo Sergio Almeida	Bettina Buth	Laurent Fribourg
Matthias Anlauff	Jens Bæk Jørgensen	Carlo Furia
Alvaro Arenas	Jacques Carette	Peter Gorm Larsen
Alexei Barantsev	David Carrington	Jean Goubault-Larrecq
Luis Barbosa	Arindam Chakrabarti	Adriaan de Groot
Leonor Barroca	Michel Chaudron	Stefan Gruner
Hubert Baumeister	Chunqing Chen	Moritz Hammer
Marek A. Bednarczyk	Jacek Chrzęszcz	Ping Hao
Maurice ter Beek	David Clark	Neil Henderson
Axel Belinfante	Joey Coleman	Martijn Hendriks
Dirk Beyer	Phil Cook	Thai Son Hoang
Machiel van der Bijl	Véronique Cortier	Martin Hofmann
Henrik Bohnenkamp	Jorge Cuellar	Jozef Hooman
Pontus Boström	Roberto Delicata	Dang Van Hung
Ahmed Bouajjani	Dubravka Ilic	Wilson Ifill
Patricia Bouyer	Bruno Dutertre	Ryszard Janicki
Folker den Braber	Neil Evans	Tomasz Janowski
Laura Brandan Briones	Alessandro Fantechi	Einar Broch Johnsen
Phil Brooke	Gianluigi Ferrari	Wolfram Kahl
Roberto Bruni	Paul Fischer	Alexander Kamkin
Hans Bruun	Oana Florescu	Ridha Khedri

Victor Khomenko
 Alexander Knapp
 Erwin van der Koogh
 Evgeny Kornychkin
 Piotr Kosiuczenko
 Fred Kröger
 Steve Kremer
 Victor Kuliamin
 Alexander Kurz
 Linas Laibinis
 Christian Lange
 Rom Langerak
 François Laroussinie
 Diego Latella
 Timo Latvala
 Christian Lengauer
 Yuan Fang Li
 Quan Long
 Mass Soldal Lund
 Volkmar Lotz
 Hans Henrik Løvengreen
 Tom Lysemose
 Qaisar Ahmad Malik
 Tiziana Margaria
 Nicolas Markey
 Mieke Massink
 Brian Matthews
 Franco Mazzanti
 Alistair McEwan
 Robert Meolic

Stephan Merz
 Ali Mesbah
 Tim Miller
 Leonardo de Moura
 Henry Muccini
 Damian Niwiński
 David von Oheim
 Nickolay Pakulin
 Jun Pang
 Dirk Pattinson
 Jan Peleska
 Luigia Petre
 Laure Petrucci
 Nir Piterman
 David Pitt
 Matteo Pradella
 Kees Pronk
 Axel Rauschmayer
 Atle Refsdal
 Brian Ritchie
 Markus Roggenbach
 Judith Rossebø
 Matteo Rossi
 Ragnhild Kobro Runde
 John Rushby
 Theo Ruys
 Denis Sabatier
 Hassen Saidi
 Thomas Santen
 Bernhard Schätz

Norbert Schirmer
 Aleksy Schubert
 Fredrik Seehusen
 Emil Sekerinski
 Natarajan Shankar
 Mike Shields
 Graeme Smith
 Monika Solanki
 Bjørnar Solhaug
 Jorge Sousa Pinto
 Simao Melo de Sousa
 Pieter van der Spek
 Paola Spoletini
 Mariëlle Stoelinga
 Asuman Suenbuel
 Jun Sun
 Helen Treharne
 Jan Tretmans
 Leonidas Tsiopoulos
 Irek Ulidowski
 Neeraj Verma
 Joost Visser
 Peter Visser
 Fredrik Vraalsen
 Marina Waldén
 Burkhardt Wolff
 Lu Yan
 Yuwen Yang

Sponsors

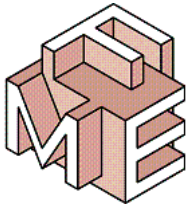


Table of Contents

Keynote Talks

Formal Aids for the Growth of Software Systems <i>Mathai Joseph</i>	1
Formal Methods and Testing: Hypotheses, and Correctness Approximations <i>Marie-Claude Gaudel</i>	2
The Natural History of Bugs: Using Formal Methods to Analyse Software Related Failures in Space Missions <i>C.W. Johnson</i>	9

Object Orientation

Modular Verification of Static Class Invariants <i>K. Rustan M. Leino, Peter Müller</i>	26
Decoupling in Object Orientation <i>Ioannis T. Kassios</i>	43
Controlling Object Allocation Using Creation Guards <i>Cees Pierik, Dave Clarke, Frank S. de Boer</i>	59
Symbolic Animation of JML Specifications <i>Fabrice Bouquet, Frédéric Dadeau, Bruno Legeard, Mark Utting</i>	75

Resource Analysis and Verification

Certified Memory Usage Analysis <i>David Cachera, Thomas Jensen, David Pichardie, Gerardo Schneider</i>	91
Compositional Specification and Analysis of Cost-Based Properties in Probabilistic Programs <i>Orieta Celiku, Annabelle McIver</i>	107
Formally Defining and Verifying Master/Slave Speculative Parallelization <i>Pierre Salverda, Grigore Roşu, Craig Zilles</i>	123

Timing and Testing

Systematic Implementation of Real-Time Models <i>Martin De Wulf, Laurent Doyen, Jean-François Raskin</i>	139
Timing Tolerances in Safety-Critical Software <i>Alan Wassyn, Mark Lawford, Xiayong Hu</i>	157
Timed Testing with TorX <i>Henrik Bohnenkamp, Axel Belinfante</i>	173
Automatic Verification and Conformance Testing for Validating Safety Properties of Reactive Systems <i>Vlad Rusu, Hervé Marchand, Thierry Jéron</i>	189

CSP, B and Circus

Adding Conflict and Confusion to CSP <i>Christie Bolton</i>	205
Combining CSP and B for Specification and Property Verification <i>Michael Butler, Michael Leuschel</i>	221
Operational Semantics for Model Checking Circus <i>Jim Woodcock, Ana Cavalcanti, Leonardo Freitas</i>	237
Control Law Diagrams in <i>Circus</i> <i>Ana Cavalcanti, Phil Clayton, Colin O'Halloran</i>	253

Security

Verification of a Signature Architecture with HOL-Z <i>David Basin, Hironobu Kuruma, Kazuo Takaragi, Burkhart Wolff</i> . . .	269
End-to-End Integrated Security and Performance Analysis on the DEGAS Choreographer Platform <i>Mikael Buchholtz, Stephen Gilmore, Valentin Haenel, Carlo Montangero</i>	286
Formal Verification of Security Properties of Smart Card Embedded Source Code <i>June Andronick, Boutheina Chetali, Christine Paulin-Mohring</i>	302

Networks and Processes

A Formal Model of Addressing for Interoperating Networks <i>Pamela Zave</i>	318
An Approach to Unfolding Asynchronous Communication Protocols <i>Yu Lei, S. Purushothaman Iyer</i>	334
Semantics of BPEL4WS-Like Fault and Compensation Handling <i>Qiu Zongyan, Wang Shuling, Pu Geguang, Zhao Xiangpeng</i>	350

Abstraction, Retrenchment and Rewriting

On Some Galois Connection Based Abstractions for the Mu-Calculus <i>Dragan Bošnački</i>	366
Retrenching the Purse: Finite Sequence Numbers, and the Tower Pattern <i>Richard Banach, Michael Poppleton, Czesław Jeske, Susan Stepney</i>	382
Strategic Term Rewriting and Its Application to a VDM-SL to SQL Conversion <i>T.L. Alves, P.F. Silva, J. Visser, J.N. Oliveira</i>	399

Scenarios and Modeling Languages

Synthesis of Distributed Processes from Scenario-Based Specifications <i>Jun Sun, Jin Song Dong</i>	415
Verifying Scenario-Based Aspect Specifications <i>Emilia Katz, Shmuel Katz</i>	432
An MDA Approach Towards Integrating Formal and Informal Modeling Languages <i>Soon-Kyeong Kim, Damian Burger, David Carrington</i>	448

Model Checking

Model-Checking of Specifications Integrating Processes, Data and Time <i>Jochen Hoenicke, Patrick Maier</i>	465
Automatic Symmetry Detection for Model Checking Using Computational Group Theory <i>A.F. Donaldson, A. Miller</i>	481

On Partitioning and Symbolic Model Checking
*Subramanian Iyer, Debashis Sahoo, E. Allen Emerson,
Jawahar Jain* 497

Dynamic Component Substitutability Analysis
Natasha Sharygina, Sagar Chaki, Edmund Clarke, Nishant Sinha 512

Industry Day: Abstracts of Invited Talks

Floating-Point Verification
John Harrison 529

Preliminary Results of a Case Study: Model Checking for Advanced
Automotive Applications
*Stefan Eisler, Christian Scheidler, Bernhard Josko,
Guido Sandmann, Joachim Stroop* 533

Model-Based Testing in Practice
Alexander Pretschner 537

Testing Concurrent Object-Oriented Systems with Spec Explorer
*Colin Campbell, Wolfgang Grieskamp, Lev Nachmanson,
Wolfram Schulte, Nikolai Tillmann, Margus Veanes* 542

ASD Case Notes: Costs and Benefits of Applying Formal Methods to
Industrial Control Software
Guy H. Broadfoot 548

The Informal Nature of Systems Engineering
Gerrit Muller 552

Author Index 557