Lecture Notes in Computer Science 3582

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Springer is a part of Springer Science+Business Media

springeronline.com

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.

July 2005 John Fitzgerald, Ian Hayes, Andrzej Tarlecki

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 Airchinnigh, 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 Wassyng, McMaster University, Canada
Martin Wirsing, Ludwig-Maximilians-Universität, München, Germany

Referees

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

Victor Khomenko
Alexander Knapp
Erwin van der Koogh
Evgeny Kornykhin
Piotr Kosiuczenko
Fred Kröger
Steve Kremer
Victor Kuliamin
Alexander Kurz
Linas Laibinis
Christian Lange
Rom Langerak
Franiçois 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
Burkhart Wolff
Lu Yan
Yuwen Yang

Sponsors

FME
SAP®
CSR
BCS FACS

Table of Contents

Keynote Talks

Object Orientation

Resource Analysis and Verification

Timing and Testing

CSP, B and Circus

Security

Networks and Processes

Abstraction, Retrenchment and Rewriting

Scenarios and Modeling Languages

Model Checking

Industry Day: Abstracts of Invited Talks