Lecture Notes in Computer Science 2391

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

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

Lars-Henrik Eriksson
Peter Alexander Lindsay (Eds.)

FME 2002: Formal Methods – Getting IT Right

International Symposium of Formal Methods Europe
Copenhagen, Denmark, July 22-24, 2002
Proceedings

Springer

Series Editors

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

Volume Editors

Lars-Henrik Eriksson
Uppsala University, Department of Information Technology
P.O. Box 337, 751 05 Uppsala, Sweden
E-mail: lhe@csd.uu.se

Peter Alexander Lindsay
The University of Queensland, Software Verification Research Centre
Queensland 4072, Australia
E-mail: Peter.Lindsay@svrc.uq.edu.au

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Formal methods - getting IT right : proceedings / FME 2002, International Symposium of Formal Methods Europe, Copenhagen, Denmark, July 22 - 24, 2002. Lars-Henrik Eriksson ; Peter Alexander Lindsay (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2391)
ISBN 3-540-43928-5

CR Subject Classification (1998): F.3, D.2, D.3, D.1, J.1, K.6, F.4.1

ISSN 0302-9743
ISBN 3-540-43928-5 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

Printed in Germany

Typesetting: Camera-ready by author, data-conversion by PTP-Berlin, Stefan Sossna e.K.
Printed on acid-free paper SPIN: 10873502 06/3142 5 4 3 2 1 0

Preface

This volume contains the proceedings of the 2002 symposium Formal Methods Europe (FME 2002). The symposium was the 11^{th} in a series that began with a VDM Europe symposium in 1987. The symposia are traditionally held every 18 months. In 2002 the symposium was held at the University of Copenhagen, as part of the 2002 Federated Logic Conference (FLoC 2002), which brought together in one event seven major conferences related to logic in computer science, as well as their affiliated workshops, tutorials, and tools exhibitions.

Formal Methods Europe (www.fmeurope.org) is an independent association which aims to stimulate the use of, and research on, formal methods for software development. FME symposia have been notably successful in bringing together a community of users, researchers, and developers of precise mathematical methods for software development.

The theme of FME 2002 was "Formal Methods: Getting IT Right". The double meaning was intentional. On the one hand, the theme acknowledged the significant contribution formal methods can make to Information Technology, by enabling computer systems to be described precisely and reasoned about with rigour. On the other hand, it recognized that current formal methods are not perfect, and further research and practice are required to improve their foundations, applicability, and effectiveness.

FME 2002 covered many aspects of the use of formal methods for development of software in many different application areas. As with previous FME symposia, FME 2002 covered a wide range of activities, from development of fundamental theory of description and reasoning, to particulars of practice and experience.

A total of 31 papers were accepted out of 95 submissions from 30 countries, half of which are outside Europe, making this a truly international event. In addition to authors of submitted papers, Natarajan Shankar, Anthony Hall, and David Basin were invited to give keynote presentations at the symposium.

A symposium session on Semantics and Logic was dedicated to the memory of John Dawes, who was a founding member of VDM Europe and a long-time active contributor to FME.

May 2002 Lars-Henrik Eriksson, Peter Lindsay

Organization

FME 2002 was organized by Formal Methods Europe and the third Federated Logic Conference (FLoC 2002). It was hosted jointly by the IT University of Copenhagen, the Technical University of Denmark, and the University of Copenhagen. We would like to thank the FME Board (John Fitzgerald, Nico Plat, and Kees Pronk) for their support, and the FLoC Organizing Committee for making local arrangements. Moshe Vardi was FLoC General Chair and Neil Jones was FLoC Conference Chair. We particularly thank Henning Makholm, Andrzej Filinski, and Sebastian Skalberg of the FLoC Local Committee for their help in organizing the web pages, the printed program, and the tool demonstration facilities.

Organizing Committee

Organizing Chair:	Dines Bjørner (Technical University of Denmark)
Program Co-chairs:	Lars-Henrik Eriksson (Industrilogik, Sweden)
	Peter Lindsay (University of Queensland, Australia)
Tool Demonstrations:	Paul Mukherjee
	(Systematic Software Engineering A/S, Denmark)

Program Committee

Bernhard Aichernig	Graz University of Technology, Austria
Juan Bicarregui	Rutherford Appleton Laboratory, UK
Ernie Cohen	Microsoft Research, Cambridge, UK
Ben Di Vito	NASA Langley Research Center, USA
Cindy Eisner	IBM Haifa Research Laboratory, Israel
Lars-Henrik Eriksson (co-chair)	Industrilogik, Sweden
John Fitzgerald	Transitive Technologies Ltd, UK
Jim Grundy	Intel Corporation, USA
Yves Ledru	IMAG Grenoble, France
Peter Lindsay (co-chair)	University of Queensland, Australia
Markus Montigel	University of New Orleans, USA
Richard Moore	IFAD, Denmark
Tobias Nipkow	Technische Universität München, Germany
Colin O'Halloran	QinetiQ, UK
Jose Oliveira	Universidade do Minho, Portugal
Nico Plat	West Consulting, The Netherlands
Jeannette Wing	Carnegie Mellon University, USA
Jim Woodcock	University of Kent, UK
Joakim von Wright	Åbo Akademi University, Finland
Pamela Zave	AT&T Laboratories, USA

External Referees

All submitted papers were peer reviewed by at least three referees. In addition to the Program Committee, the following people contributed reviews:

Referees

Parosh Aziz Abdulla
James M Armstrong
Clemens Ballarin
Luís S. Barbosa
Sharon Barner
Leonor Barroca
Shoham Ben-David
Pierre Berlioux
Didier Bert
Eerke Boiten
Roland Bol
Gregory Bond
Michael Butler
Martin Büchi
Orieta Celiku
Michel Chaudron
David Clark
Pieter Cuipers
Anat Dahan
John Derrick
Jeremy Dick
Theo Dimitrakos
Lydie du Bousquet
Steve Dunne
Sophie Dupuy-Chessa
Andy Evans
João M. Fernandes
Jean-Claude Fernandez
Arnaud Fevrier
Colin Fidge
Daniel Geist
Anna Gerber
Rob Gerth
Stephen Gilmore
Stefan Gruner
Alan Hartman
David Hemer
Dang Van Hung
Tomasz Janowski
He Jifeng
Robert B. Jones
Jan Jürjens
Steve King
Andre S. E. Koster
Linas Laibinis
K. Lano
Johan Lilius
Zhiming Liu
Anthony MacDonald
Ricardo J. Machado
Brian Matthews
C. A. Middelburg
Anna Mikhailova
Tim Miller
N. Moffat
Paul Mukherjee
Markus Müller-Olm
Marco Nijdam
John O'Leary
Jeff Z. Pan
P. K. Pandya
Joachim Parrow
Stephen Paynter
Paul Pettersson
Sibylle Peuker
Andrej Pietschker
Ivan Porres
Marie-Laure Potet
Viorel Preoteasa
Alex Pretschner
Kees Pronk
Xu Qiwen
S Riddle
Brian Ritchie
Ken Robinson
Alexander Romanovsky
Kaisa Sere
W. Simmonds
David Sinclair
Graeme Smith
M. A. Smith
Baruch Sterin
Martin Strecker
Kim Sunesen
Francis Tang
Jan Tretmans
John Turner
Rachel Tzoref
Shmuel Ur
Gertjan van Oosten
Marcel Verhoef
Arjan Vermeij
M. Voorhoeve
Jos Vrancken
Hagen Völzer
Marina Waldén
Heike Wehrheim
Markus Wenzel
Alan Cameron Wills
Guido Wimmel
Kirsten Winter
Jin Yang
Emmanuel Zarpas

Table of Contents

Little Engines of Proof 1
Natarajan Shankar

Automated Boundary Testing from Z and B 21
Bruno Legeard, Fabien Peureux, Mark Utting

Improvements in Coverability Analysis 41
Gil Ratsaby, Baruch Sterin, Shmuel Ur

Heuristic-Driven Test Case Selection from Formal Specifications. A Case Study 57
Juan C. Burguillo-Rial, Manuel J. Fernández-Iglesias, Francisco J. González-Castaño, Martín Llamas-Nistal

UniTesK Test Suite Architecture 77
Igor B. Bourdonov, Alexander S. Kossatchev, Victor V. Kuliamin, Alexander K. Petrenko

Hoare Logic for NanoJava: Auxiliary Variables, Side Effects, and Virtual Methods Revisited 89
David von Oheimb, Tobias Nipkow

Do Not Read This 106
Juan C. Bicarregui

Safeness of Make-Based Incremental Recompilation 126
Niels Jørgensen

An Algorithmic Approach to Design Exploration 146
Sharon Barner, Shoham Ben-David, Anna Gringauze, Baruch Sterin, Yaron Wolfsthal

Mechanical Abstraction of CSP$_Z$ Processes 163
Alexandre Mota, Paulo Borba, Augusto Sampaio

Verifying Erlang Code: A Resource Locker Case-Study 184
Thomas Arts, Clara Benac Earle, John Derrick

Towards an Integrated Model Checker for Railway Signalling Data 204
Michael Huber, Steve King

Correctness by Construction: Integrating Formality into a Commercial Development Process 224
Anthony Hall

VAlloy – Virtual Functions Meet a Relational Language 234
Darko Marinov, Sarfraz Khurshid

Verification Using Test Generation Techniques 252
Vlad Rusu

Formal Specification and Static Checking of Gemplus' Electronic Purse Using ESC/Java 272
Néstor Cataño, Marieke Huisman

Development of an Embedded Verifier for Java Card Byte Code Using Formal Methods 290
Ludovic Casset

Deriving Cryptographically Sound Implementations Using Composition and Formally Verified Bisimulation 310
Michael Backes, Christian Jacobi, Birgit Pfitzmann

Interference Analysis for Dependable Systems Using Refinement and Abstraction 330
Claus Pahl

The Formal Classification and Verification of Simpson's 4-Slot Asynchronous Communication Mechanism 350
N. Henderson, S.E. Paynter

Timing Analysis of Assembler Code Control-Flow Paths 370
C.J. Fidge

Towards OCL/RT 390
María Victoria Cengarle, Alexander Knapp

On Combining Functional Verification and Performance Evaluation Using CADP 410
Hubert Garavel, Holger Hermanns

The Next 700 Synthesis Calculi 430
David Basin

Synthesizing Certified Code 431
Michael Whalen, Johann Schumann, Bernd Fischer

Refinement in *Circus* 451
Augusto Sampaio, Jim Woodcock, Ana Cavalcanti

Forward Simulation for Data Refinement of Classes 471
Ana Cavalcanti, David A. Naumann

A Formal Basis for a Program Compilation Proof Tool 491
Luke Wildman

Property Dependent Abstraction of Control Structure for Software Verification 511
Thomas Firley, Ursula Goltz

Closing Open SDL-Systems for Model Checking with DTSpin 531
Natalia Ioustinova, Natalia Sidorova, Martin Steffen

A Generalised Sweep-Line Method for Safety Properties 549
Lars Michael Kristensen, Thomas Mailund

Supplementing a UML Development Process with B 568
Helen Treharne

Semantic Web for Extending and Linking Formalisms 587
Jin Song Dong, Jing Sun, Hai Wang

A Language for Describing Wireless Mobile Applications with Dynamic Establishment of Multi-way Synchronization Channels 607
Takaaki Umedu, Yoshiki Terashima, Keiichi Yasumoto, Akio Nakata, Teruo Higashino, Kenichi Taniguchi

Author Index 625