Lecture Notes in Computer Science 2021

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

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

José Nuno Oliveira Pamela Zave (Eds.)

FME 2001: Formal Methods for Increasing Software Productivity

International Symposium of Formal Methods Europe
Berlin, Germany, March 12-16, 2001
Proceedings

Springer

Volume Editors

José Nuno Oliveira
University of Minho, Computer Science Department
Campus de Gualtar, 4700-320 Braga, Portugal
E-mail: jno@di.uminho.pt

Pamela Zave
AT&T Laboratories – Research
180 Park Avenue, Florham Park, New Jersey 07932, USA
E-mail: pamela@research.att.com

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Formal methods for increasing software productivity : proceedings /
FME 2001, International Symposium of Formal Methods Europe, Berlin,
Germany, March 12 - 16, 2001. José Nuno Oliveira ; Pamela Zave (ed.).
- Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ;
Milan ; Paris ; Singapore ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 2021)
ISBN 3-540-41791-5

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

ISSN 0302-9743
ISBN 3-540-41791-5 Springer-Verlag Berlin Heidelberg New York

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

http://www.springer.de

Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna
Printed on acid-free paper SPIN: 10782329 06/3142 5 4 3 2 1 0

Preface

FME 2001 is the tenth in a series of meetings organized every eighteen months by Formal Methods Europe (FME), an independent association whose aim is to stimulate the use of, and research on, formal methods for software development. It follows four VDM Europe Symposia, four other Formal Methods Europe Symposia, and the 1999 World Congress on *Formal Methods in the Development of Computing Systems*. These meetings have been notably successful in bringing together a community of users, researchers, and developers of precise mathematical methods for software development.

FME 2001 took place in Berlin, Germany and was organized by the Computer Science Department of the Humboldt-Universität zu Berlin. The theme of the symposium was *Formal Methods for Increasing Software Productivity*. This theme recognizes that formal methods have the potential to do more for industrial software development than enhance software quality – they can also increase productivity at many different points in the software life-cycle.

The importance of the theme is borne out by the many contributed papers showing how formal methods can make software development more efficient. There is an emphasis on tools that find errors automatically, or with relatively little human effort. There is also an emphasis on the use of formal methods to assist with critical, labor-intensive tasks such as program design and test-case generation.

The many application areas addressed in the various parts of the symposium (tutorials, workshops, contributed papers, and invited papers) include smart cards, avionic and satellite computers, financial contracts, E-commerce, middleware, security, telecommunications, and the FireWire standard. Many contributions involve multi-disciplinary teams of researchers coming from both industry and academia. We are pleased to see this evidence of the spreading influence of formal methods.

In addition to the 32 papers selected for presentation by the program committee (out of 72 submissions involving authors from 25 countries), this volume contains the abstracts of three invited talks: *Lightweight Formal Methods*, by Daniel Jackson (Laboratory for Computer Science, MIT); *A Programming Model for Wide-Area Computing*, by Jayadev Misra (University of Texas at Austin); and *Composing Contracts: An Adventure in Financial Engineering* by Simon Peyton Jones (Microsoft Research Ltd).

January 2001

José Nuno Oliveira
Pamela Zave

Acknowledgements

We are very grateful to the members of the program committee and their referees for their care and diligence in reviewing the submitted papers. We are also grateful to the local organizers and the sponsoring institutions.

Program Committee

Eerke Boiten (UK)
Rick Butler (USA)
Lars-Henrik Eriksson (Sweden)
John Fitzgerald (UK)
Peter Gorm Larsen (Denmark)
Yves Ledru (France)
Dominique Méry (France)
Jayadev Misra (USA)
Richard Moore (Macau)
Friederike Nickl (Germany)
Tobias Nipkow (Germany)
José N. Oliveira (co-chair, Portugal)
Paritosh Pandya (India)
Nico Plat (The Netherlands)
Amir Pnueli (Israel)
Augusto Sampaio (Brazil)
Steve Schneider (UK)
Jim Woodcock (UK)
Pamela Zave (co-chair, USA)

Organizing Committee

Birgit Heene
Stefan Jähnichen (co-chair)
Axel Martens
Wolfgang Reisig (co-chair)
Thomas Urban
Tobias Vesper

Sponsoring Institutions

The generous support of the following companies and institutions is gratefully acknowledged:

Humboldt-Universität zu Berlin
GMD FIRST
Formal Methods Europe
Universidade do Minho
DaimlerChrysler AG
WIDIS GmbH Berlin
WISTA Management GmbH

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 quality of the symposium would have suffered. To the best of our knowledge the list below is accurate. We apologize for any omissions or inaccuracies.

Will Adams
Carlos Bacelar Almeida
Rajeev Alur
Tamarah Arons
Roberto Souto Maior de Barros
Pierre Berlioux
Didier Bert
Juan Bicarregui
Lynne Blair
Roland Bol
Paulo Borba
Lydie du Bousquet
Max Breitling
Dominique Cansell
Ana Cavalcanti
Michel Chaudron
David Cohen
Ernie Cohen
Jonathan Draper
Sophie Dupuy-Chessa
Peter van Eijk
Loe Feijs
Jean-Claude Fernandez
Dana Fisman
D. Galmiche
Max Geerling
Chris George
P. Gibson
N. Goga
Jan Friso Groote
Jan Haveman
Ian Hayes
Maritta Heisel
Rolf Hennicker
Dang Van Hung
Tomasz Janowski
He Jifeng
Adrian Johnstone
Cliff B. Jones
Rajeev Joshi
Charanjit S. Jutla
Alexander Knapp
Nora Koch
Izak van Langevelde
Antónia Lopes
Gavin Lowe
Panagiotis Manolios
Andrew Martin
Stephan Merz
Anna Mikhailova
Oliver Moeller
Alexandre Mota
Paul Mukherjee
Kedar S. Namjoshi
David Naumann
George Necula
Gertjan van Oosten
Stephen Paynter
Andrej Pietschker
Nir Piterman
Marie-Laure Potet
Alexander Pretschner
Kees Pronk
Antonio Ravara
Jean-Luc Richier
Steve Riddle
Jan Rogier
Nick Rossiter
Stefan Römer
Thomas Santen
João Saraiva
Emil Sekerinski
Kaisa Sere
Elad Shahar
Ofer Shtrichman
Kim Sunesen
Hans Tonino
Richard Trefler
Alexandre Vasconcelos
Marcel Verhoef
Vladimir Zadorozhny
Irfan Zakiuddin
Lenore Zuck

Tutorials and Workshops

The following tutorials were scheduled for the two days preceding the research symposium:

SDL 2001 — J. Fischer, Andreas Prinz, and Eckhardt Holz (Humboldt-Universität zu Berlin and DResearch Digital Media Systems GmbH)

Modeling for Formal Methods — Mícheál Mac an Airchinnigh, Andrew Butterfield, and Arthur Hughes (University of Dublin)

From UML to Z, Support for Requirements Engineering with RoZ — Yves Ledru and Sophie Dupuy (LSR/IMAG)

Beyond Model Checking: Formal Specification and Verification of Practical Mission-Critical Systems — Ramesh Bharadwaj (Naval Research Laboratory, USA)

We are grateful to all those who kindly submitted tutorial proposals. In addition, two international workshops were co-located with the symposium tutorials:

First International Workshop on Automated Verification of Infinite-State Systems (AVISS'01) — organized by Ramesh Bharadwaj (Naval Research Laboratory, USA) and Steve Sims (Reactive-Systems, Inc.)

Formal Approaches to the IEEE 1394 (FireWire) Identify Protocol — organized by Carron Shankland, Savi Maharaj (University of Stirling), and Judi Romijn (University of Nijmegen).

We thank the organizers of these events for their interest in sharing the atmosphere of the symposium.

Table of Contents