

Lecture Notes in Computer Science

670

Edited by G. Goos and J. Hartmanis

Advisory Board: W. Brauer D. Gries J. Stoer



J.C.P. Woodcock P.G. Larsen (Eds.)

FME '93: Industrial-Strength Formal Methods

First International Symposium
of Formal Methods Europe
Odense, Denmark, April 19-23, 1993
Proceedings

Springer-Verlag

Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Series Editors

Gerhard Goos
Universität Karlsruhe
Postfach 69 80
Vincenz-Priessnitz-Straße 1
W-7500 Karlsruhe, FRG

Juris Hartmanis
Cornell University
Department of Computer Science
4130 Upson Hall
Ithaca, NY 14853, USA

Volume Editors

James C. P. Woodcock
Oxford University Computing Laboratory, Programming Research Group
11 Keble Road, Oxford OX1 3QD, U.K.

Peter G. Larsen
The Institute of Applied Computer Science (IFAD)
Forskerparken 10, 5230 Odense M, Denmark

CR Subject Classification (1991): D.1-2, F.3.1, J.1

ISBN 3-540-56662-7 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-56662-7 Springer-Verlag New York Berlin Heidelberg

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 Berlin Heidelberg 1993
Printed in Germany

Typesetting: Camera ready by author/editor
Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
45/3140-543210 - Printed on acid-free paper

Preface

In September 1988 I attended the second *VDM Symposium* in Dublin, and suggested, first to Cliff Jones, and then to Dines Bjørner, that we should widen the scope of the Symposium to include the Z notation. I was pushing at an open door, and the next symposium, held in Kiel in April 1990, was devoted to VDM and Z. This process of widening the scope of the symposium continued with the next in the series: it was held in Noordwijkerhout in October 1991, and covered Formal Software Development Methods.

This trend towards a broader range of methods also reflects a change that has been made in the organisation that lies behind the series. All four VDM symposia were organised by VDM Europe, an advisory board sponsored by the Commission of the European Communities. The board's working group was made up from academia and industry, and met several times each year to discuss the industrial usage of model-oriented formal methods, most usually those connected with VDM (including RAISE and MetaSoft). This board has evolved into Formal Methods Europe, and this volume contains the proceedings of its first symposium.

The last few years have borne witness to the remarkable diversity of formal methods, with applications to sequential and concurrent software, to real-time and reactive systems, and to hardware design. In that time, many theoretical problems have been tackled and solved, and many continue to be worked upon. Yet it is by the suitability of their industrial application and the extent of their usage that formal methods will ultimately be judged. This symposium will focus on *The Application of Industrial-Strength Formal Methods*. We have encouraged papers to address the difficulties of scaling their techniques up to industrial-sized problems, and of their suitability in the work-place, and to discuss techniques that are formal (that is, they have a mathematical basis), and that are industrially applicable. Papers tackling theoretical issues were much encouraged, providing that they contained a justification of the practical advantages that follow. We received over 140 submissions of various kinds, with a strong representation from outside Europe, in particular Australia and the United States. We invited three speakers to address the symposium, and accepted seven industrial usage reports and 32 papers, complemented by eight tutorials on various formal methods, and an exhibition of over 20 formal methods tools.

This volume has four parts to it: the contributions of invited speakers; industrial reports; papers; and descriptions of the tools exhibited. We have three distinguished invited speakers: Professor Cliff Jones, Professor Willem-Paul de Roever, and Peter Lupton (whose talk is not recorded in the proceedings). The industrial usage reports describe practical experiences from the applications of formal methods in challenging industrial environments. The papers cover a wide variety of methods and notations. We have modal logic, the refinement calculus, RAISE, CCS, Petri Nets, VDM, Z, LOTOS, OBJ, Sprint, and B, and deal with the combination of formal and informal techniques, object-orientation, applications to high-assurance systems involving both safety and security, and papers on theory and its relevance to practice.

J.C.P.Woodcock
Oxford, February 1993

Acknowledgments

Many people have contributed to the planning, organisation and success of FME'93.

Programme Committee

Jim Woodcock (PC Chairman)
 Peter Gorm Larsen (OC Liaison)
 J.-R. Abrial
 Tim Denvir
 Eugene Dürr
 Ian Hayes
 Steve King
 Hans Langmaack
 Mícheál Mac an Airchinnigh
 Kees Middelburg
 Søren Prehn
 Hans Toetenel

Organising Committee

Peter Gorm Larsen (OC Chairman)
 Poul Bøgh Lassen (Tools Exhibition)
 Michael Andersen
 Kees de Bruin
 René Elmstrøm
 Søren Larsen
 Erik Toubro Nielsen
 Henrik Aagaard Pedersen

Local Organisers

Kirsten Johansen
 Bitten Filstrup
 Lone Weidemann
 Susanne Rasmussen

} KongresBureau Fyn

In addition, the invaluable contributions of the following should be acknowledged: Alejandro Moya, CEC, for his continued support to Formal Methods Europe; Alfred Hofmann of Springer-Verlag for their continued interest in publishing these proceedings; Miss Frances Page for her expert assistance in helping to organise submitted papers and referees' reviews; Steve King for his assistance in solving (almost all) the \LaTeX and postscript problems with the proceedings.

The final addition to the conference programme were the presentations by a number of European projects on formal specification and design. We wish to thank all these projects for their interest in FME'93.

We would also like to thank Odense Teknikum for being so flexible that it has been possible to host the FME'93 symposium there.

External Referees

All submitted papers—whether accepted or rejected—were refereed by the programme committee members and a number of external referees. This symposium would not have been possible without their voluntary and dedicated work.

Michael Andersen	Derek Andrews	Rob Arthan
Rudolf Berghammer	Wiet Bouma	Jonathan Bowen
Stephen Brien	Manfred Broy	David Carrington
Flemming Damm	Werner Damm	Tony Darlison
Roger Duke	Hans Dieter Ehrich	René Elmstrøm
John Fitzgerald	Catriona Fox	Jacob Frost
Martin Fränzle	Jean Goubault	Christian Gram
Jan Friso Groote	Lindsay Groves	Anthony Hall
Bo Stig Hansen	Friedrich Wilhelm von Henke	Mike Hinchey
Ronald Huijsman	Kees Huizin	Dave Jackson
Roger Jones	Jan van Katwijk	Peter Kearney
Trevor King	Hans Kloosterman	Peter Kluit
Hans Jörg Kreowski	Bernd Krieg-Brückner	Kevin Lano
Ole Bjerg Larsen	Søren Larsen	Poul Bøgh Lassen
George Leih	Peter Lindsay	Hans Henrik Løvengreen
Wayne Luk	Brendan Mahony	Derek Mannering
Andrew Martin	Swapan Mitra	Carroll Morgan
Maurice Naftalin	Manfred Nagl	John Nicholls
Ernst Rüdiger Olderog	Jens Palsberg	Peter Pepper
Nico Plat	Ben Potter	Kees Pronk
Anders P. Ravn	Joy Reed	Wolfgang Reisig
Hans Rischel	Gordon Rose	Jeff Sanders
Steve Schneider	Danny de Schreye	Karen Seidel
Robin Sharp	Jane Sinclair	Jens Ulrik Skakkebæk
Arne Skou	Gregor Snelting	Rud Sommerhalder
Jan Springintveld	John Staples	Jørgen Staunstrup
Werner Stephan	Andrew Stevens	Werner Struckmann
Mario Südholt	Paul Taylor	Hans Tonino
Mark Utting	Hugo Velthuisen	Friedrich Vogt
Nigel Ward	Jim Welsh	Han Zuidweg

We apologise if, inadvertently, we have omitted a referee from the above list. To the best of our knowledge the list is accurate.

Symposium Sponsors

The symposium would not have been possible without the kind support and financial assistance of the associations and corporations listed below:

Scandinavian Airlines System (SAS)
 Odense Steel Shipyard Ltd.
 Deutsche System Technik
 Fyns Telefon
 Praxis
 Lloyd's Register
 DDC International
 Space Software Italia
 Computer Resources International (CRI)
 ICL Data A/S (SUN Division)

Oxford University and The Institute of Applied Computer Science (IFAD) have both been most generous in their support of the symposium.

Tutorial Programme

Copies of this material will be handed out to all participants in the tutorial part of the symposium.

The tutorials of FME'93 present a comprehensive account of the current state of the art. The chosen tutorials have been particularly selected to fit the subtitle of the symposium: *Industrial-strength Formal Methods*. We would like to thank all tutors for their kind willingness to give these tutorials.

The tutorials are:

Functional Programming	<i>Phil Wadler</i>
Coloured Petri Nets	<i>Kurt Jensen</i>
Data Refinement	<i>Tim Clement</i>
CCS with Tool Support	<i>Kim G. Larsen</i>
Proof in Z with Tool Support	<i>Roger Jones</i>
LOTOS with Tool Support	<i>Jeroen Schot</i>
Prototype Verification System (PVS)	<i>John Rushby</i>
Provably Correct Systems (ProCoS)	<i>Anders P. Ravn</i>

Table of Contents

Invited Lectures

Reasoning about Interference in an Object-Based Design Method 1
C.B. Jones

Using Relative Refinement for Fault Tolerance 19
Antonio Cau & Willem-Paul de Roever

Industrial Usage Reports

Specification and Validation of a Security Policy Model 42
Tony Boswell

Experiences from Applications of RAISE 52
B. Dandanell, Jesper Gørtz, Jan Storbank Pedersen, & Eld Zierau

Role of VDM(++) in the Development of a Real-Time Tracking and Tracing System 64
E.H. Dürr & E.M. Dusink

The Integration of LOTOS with an Object-Oriented Development Method 73
Mikael Hedlund

An Industrial Experience on LOTOS-Based Prototyping for Switching Systems Design 83
Gonzalo León, Juan C. Yelmo, Carlos Sánchez, F. Javier Carrasco,
& Juan J. Gil

Towards an Implementation-oriented Specification of TP Protocol in LOTOS ... 93
Ing Widya & Gert-Jan van der Heijden

Papers

A Metalanguage for the Formal Requirement Specification of Reactive Systems 110
Egidio Astesiano & Gianna Reggio

Model Checking in Practice: the T9000 Virtual Channel Processor 129
Geoff Barrett

Algorithm Refinement with Read and Write Frames 148
Juan Bicarregui

Invariants, Frames and Postconditions: a Comparison of the VDM and B Notations 162
Juan Bicarregui & Brian Ritchie

The Industrial Take-up of Formal Methods in Safety-Critical and Other Areas: A Perspective 183
Jonathan Bowen & Victoria Stavridou

<i>A Proof Environment for Concurrent Programs</i>	196
Naïma Brown & Dominique Mery	
<i>A VDM* study of Fault-Tolerant Stable Storage Towards a Computer Engineering Mathematics</i>	216
Andrew Butterfield	
<i>Applications of Modal Logic for the Specification of Real-Time Systems</i>	235
Liang Chen & Alistair Munro	
<i>Formal Methods Reality Check: Industrial Usage</i>	250
Dan Craigen, Susan Gerhart, & Ted Ralston	
<i>Automating the Generation and Sequencing of Test Cases from Model-Based Specifications</i>	268
Jeremy Dick & Alain Faivre	
<i>The Parallel Abstract Machine: A Common Execution Model for FDTs</i>	285
Guillaume Doumenc Jean-Francois Monin	
<i>Generalizing Abadi & Lamport's Method to Solve a Problem Posed by A. Pnueli</i>	294
Kai Engelhardt & Willem-Paul de Roever	
<i>Real-Time Refinement</i>	314
Colin Fidge	
<i>Different FDTs Confronted with Different ODP-Viewpoints of the Trader</i>	332
Joachim Fischer, Andreas Prinz, & Andreas Vogel	
<i>On the Derivation of Executable Database Programs from Formal Specifications</i>	351
T. Günther, Klaus-Dieter Schewe, & Ingrid Wetzel	
<i>A Concurrency Case Study using RAISE</i>	367
Anne Haxthausen & Chris George	
<i>Specifying a Safety-Critical Control System in Z</i>	388
Jonathan Jacky	
<i>An Overview of the SPRINT Method</i>	403
H.B.M. Jonkers	
<i>Application of Composition Development Method for Definition of SYNTHESIS Information Resource Query Language Semantics</i>	428
Leonid Kalinichenko, Nikolaj Nikitchenko, & Vladimir Zadorozhny	
<i>Verification Tools in the Development of Provably Correct Compilers</i>	442
M.R.K. Krishna Rao, P.K. Pandya, & R.K. Shyamasundar	
<i>Encoding W: A Logic for Z in 2OBJ</i>	462
Andrew Martin	

<i>Formal Verification for Fault-Tolerant Architectures: Some Lessons Learned</i> ...	482
Sam Owre, John Rushby, Natarajan Shankar, & Friedrich von Henke	
<i>Conformity Clause for VDM-SL</i>	501
Graeme I. Parkin & Brian Wichmann	
<i>Process Instances in LOTOS Simulation</i>	521
Simon Pickin, Yan Yang, Wiet Bouma, Sylvie Simon, & Tanja de Groot	
<i>The SAZ Project: Integrating SSADM and Z</i>	541
Fiona Polack, Mark Whiston, & Keith Mander	
<i>Maintaining Consistency Under Changes to Formal Specifications</i>	558
Kelvin J. Ross & Peter A. Lindsay	
<i>An EVES Data Abstraction Example</i>	578
Mark Saaltink, Sentot Kromodimoeljo, Bill Pase, Dan Craigen, & Irwin Meisels	
<i>Putting Advanced Reachability Analysis Techniques Together: the "ARA" Tool</i>	597
Antti Valmari, Jukka Kemppainen, Matthew Clegg, & Mikko Levanto	
<i>Integrating SA/RT with LOTOS</i>	617
Anthony W. van der Vloedt & Kees Bogaards	
<i>Symbolic Model Checking for Distributed Real-Time Systems</i>	632
Farn Wang, Aloysius Mok, & E. Allen Emerson	
<i>Adding Specification Constructors to the Refinement Calculus</i>	652
Nigel Ward	
<i>Selling Formal Methods to Industry</i>	671
Debora Weber-Wulff	
Tool Descriptions	679
<i>ProofPower, Mural</i>	679
<i>IPTES Toolset, The Centaur-VDM environment</i>	680
<i>IFAD VDM-SL Toolbox, DST-fuzz</i>	681
<i>The LOTOS Toolbox, Centaur</i>	682
<i>DisCo, The Boyer-Moore Theorem Prover</i>	683
<i>B-Toolkit, Pet Dingo</i>	684
<i>SpecBox, Raise</i>	685
<i>ExSpect, CADiZ</i>	686
<i>Design/CPN, PVS</i>	687
<i>TAV, FDR</i>	688
<i>ForMooZ</i>	689