Lecture Notes in Computer Science 670

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

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
Ruud Sommerhalder
Jan Springintveld
John Staples
Jørgen Staunstrup
Werner Stephan
Andrew Stevens
Werner Struckmann
Mario Südholt
Paul Taylor
Hans Tonino
Mark Utting
Hugo Velthuijsen
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	*Phil Wadler*
Coloured Petri Nets	*Kurt Jensen*
Data Refinement	*Tim Clement*
CCS with Tool Support	*Kim G. Larsen*
Proof in Z with Tool Support	*Roger Jones*
LOTOS with Tool Support	*Jeroen Schot*
Prototype Verification System (PVS)	*John Rushby*
Provably Correct Systems (ProCoS)	*Anders P. Ravn*

Table of Contents

Invited Lectures

Industrial Usage Reports

Papers