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 6980
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


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 | Organising Committee |
|---|---|
| Jim Woodcock (PC Chairman) | Peter Gorm Larsen (OC Chairman) |
| Peter Gorm Larsen (OC Liaison) | Poul Bøgh Lassen (Tools Exhibition) |
| J.-R. Abrial | Michael Andersen |
| Tim Denvir | Kees de Bruin |
| Eugene Dürr | René Elmstrøm |
| Ian Hayes | Søren Larsen |
| Steve King | Erik Toubro Nielsen |
| Hans Langmaack | Henrik Aagaard Pedersen |
| Mícheál Mac an Airchinnigh | |
| Kees Middelburg | |
| Søren Prehn | |
| Hans Toetenel | |

**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

# Reasoning about Interference in an Object-Based Design Method

C. B. Jones

Department of Computer Science
Manchester University, M13 9PL, UK
cbj@cs.man.ac.uk

**Abstract.** The property of a (formal) development method which gives the development process the potential for productivity is *compositionality*; compositional development methods for concurrent systems are elusive because of *interference*. A companion paper shows how object-based concepts can be used to provide a designer with control over interference and proposes a transformational style of development in which concurrency is introduced only in the final stages of design. That approach relies on restrictions to the object graphs which can arise and works for systems which involve limited interference. The current paper discusses the problems of interference and shows how a suitable logic can be used to reason – during design – about those systems where interference plays an essential role. Here again, concepts are used in the design notation which are taken from object-oriented languages since they offer control of granularity and ways of pinpointing interference. A further paper is in preparation which discusses the semantics of the object-based design notation.



## 1 Introduction

Development of any large computer system is difficult but formal methods like VDM have been shown to help control the development process – and provide useful documentation – of sequential systems. A method which permits one step of design to be justified before proceeding to the next stage of design is said to be compositional: compositional formal methods can contribute to the productivity of the design task by reducing the 'scrap and rework' inherent in approaches which fail to detect mistakes until long after they are made.

Clearly, an attack on the problem of developing concurrent systems should preserve what is usable from methods aimed at sequential systems; a companion paper [Jon93a] shows how some classes of concurrent programs can be designed by adding a transformational step to development using sequential methods like data reification and operation decomposition (see also Section 3 below). Where the methods themselves are not adequate, at least the lessons from sequential development should be taken over. Paramount among these is the need for compositionality. But years of research (cf. [dR85, HdR86]) has shown that finding compositional development methods for concurrent systems has proved extremely difficult. In the case of shared-variable programs interference manifests itself by processes reading and changing a collection of variables (state) which they have in common. Such interference makes the conventional view of extensional denotations give way to

more complex spaces such as resumptions. Interference also invalidates conventional pre/post-condition reasoning. Section 2 reviews some earlier attempts to accommodate interference. But this is not the only problem. Interference forces a discussion of granularity which is often handled in an *ad hoc* way by declaring, for example, that assignment statements should be atomic. Related to this is the difficulty that – in the presence of interference – it is even necessary to be careful about what is meant by an assertion. These are all problems to which the current paper attempts to contribute solutions. Other difficulties of concurrency such as deadlocks and fairness remain to be tackled.

The approach taken in this – and the related papers – is to employ concepts from object-oriented programming. The general idea to obtain more tractable concurrent programs by making judicious language restrictions has a long pedigree: the development from semaphores, through conditional critical sections and monitors to languages like CSP can be seen in this light. At first sight, it is tempting to hope that notations like CSP and CCS finesse the problem of interference by abolishing states: on closer examination, it becomes clear that interfering communication can be equally troublesome. Not only are shared variables not the root of the problem, it could even be argued that process algebras are too draconian in completely abolishing states. It would appear that object-based concepts can provide a middle way (not unlike monitors [Hoa74]) where the degree of isolation (or the amount of interference permitted) can be controlled by the designer. Even the specific idea to make tractable the development of concurrent programs by using object-oriented concepts is not new and the current line owes much to the work on POOL [AR89]. The first paper in the current series [Jon93a] shows how object-based techniques limit interference; it also discusses the design notation ($\pi o \beta \lambda$) in more detail than in this paper. But a general development method for concurrent systems has to be able to cope with interference; the current paper shows how object-based concepts can be used to pinpoint and reason about interference in a way which limits the proof obligations which arise. Object-oriented languages are not a complete solution to the problems of concurrency. Indeed, this author remains unconvinced that inheritance – one of the key object-oriented concepts – is well-enough thought out to be used in any program development method. The references of object-based techniques are also open to the same abuses as more general pointers and the realization that invariants were essential to reason about the object graphs which evolve was one of the key steps in the current author's research.

Section 3 shows the sort of transformational development – usable on simple object graphs – which is discussed in more detail in [Jon93a]; Section 5 tackles the problem of interference when such simple object graphs do not suffice; Section 4 discusses the logic used. Several comments have been made about the earlier paper in this series; [Jon93b] attempts to fix the semantics of the $\pi o \beta \lambda$ design notation.

## 2 Background

There are many aspects of concurrent programs and many different problems in their development; this paper focuses on interference. It is argued above that methods of reasoning about concurrent programs must accommodate interference. To provide