Joseph M. Morris and Roger C. Shaw (Eds.)

4th Refinement Workshop


Springer-Verlag London Ltd.
Preface

This volume contains the proceedings of the 4th Refinement Workshop which was organised by the British Computer Society specialist group in Formal Aspects of Computing Science and held in Wolfson College, Cambridge, on 9-11 January, 1991. The term refinement embraces the theory and practice of using formal methods for specifying and implementing hardware and software. Most of the achievements to date in the field have been in developing the theoretical framework for mathematical approaches to programming, and on the practical side in formally specifying software, while more recently we have seen the development of practical approaches to deriving programs from their specifications. The workshop gives a fair picture of the state of the art: it presents new theories for reasoning about software and hardware and case studies in applying known theory to interesting small- and medium-scale problems. We hope the book will be of interest both to researchers in formal methods, and to software engineers in industry who want to keep abreast of possible applications of formal methods in industry.

The programme consisted both of invited talks and refereed papers. The invited speakers were Ib Sørensen, Jean-Raymond Abrial, Donald MacKenzie, Ralph Back, Robert Milne, Mike Read, Mike Gordon, and Robert Worden who gave the introductory talk. This is the first refinement workshop that solicited papers for refereeing, and despite a rather late call for papers the response was excellent. Indeed we received more good quality papers than we had room for in the programme, and so the proceedings contains a couple more papers than there were presentations at the workshop.

The organising committee consisted of Rosalind Barden (Logica Cambridge, local arrangements), Stephen Bear (Hewlett-Packard), Bernard Carre (Program Validation Ltd), Tim Denvir (Praxis and DTI, finance), Joseph Morris (Glasgow University, technical programme), Roger Shaw (Lloyds Register, chair), Jim Woodcock (PRG, Oxford), and John Wordsworth (IBM, publicity). We had support from three quarters: Logica Cambridge generously gave financial support; IBM donated a prize for the best presentation (which the participants elected to give to Ken Wood); and an army of referees kindly gave up their time to review the submitted papers without delay. Perhaps it
Preface

says something for the hope that formal methods may make a real contribution to the development of serious software that so many of these expert reviewers came from industry.

February 1991

Joseph M. Morris
Roger C. Shaw
## Contents

- The Process of Refinement: Introductory Talk to the 4th Refinement Workshop  
  *R. Worden* ................................................................. 1

- Engineering Real Software Using Formal Methods  
  *M.K.O. Lee, P.N. Scharbach and I.H. Sørensen* ............... 6

- Specialising Abstract Programs  
  *A. Gravell* ............................................................... 34

- A Refinement Case Study (Using the Abstract Machine Notation)  
  *J.R. Abrial* ............................................................. 51

- Assertional Data Reification Proofs: Survey and Perspective  
  *J. Coenen, W.-P. de Roever and J. Zwiers* .................. 97

- Formal Methods and the Sociology of Proof  
  *D. MacKenzie* .......................................................... 115

- Refinement Diagrams  
  *R.J.R. Back* ............................................................ 125

- A Case Study in Timed Refinement: A Central Heater  
  *B. Mahoney and I. Hayes* ........................................ 138

- Object Oriented Specification and Refinement  
  *P.J. Whysall and J.A. McDermid* ................................ 150

- The Ecology of Class Refinement  
  *C. Bailes and R. Duke* ............................................... 185

- Transforming Axioms for Data Types into Sequential Programs  
  *R. Milne* ................................................................. 197
Contents

Refinement of Two Graph Problems
D.A. Carrington and K.A. Robinson .............................................. 241

CSP and Timewise Refinement
G.M. Reed, A.W. Roscoe and S.A. Schneider ................................ 258

The Elusive Software Refinery: A Case Study in Program Development
K.R. Wood ....................................................................................... 281

A Theory of State-based Parallel Programming: Part 1
Q. Xu and J. He .............................................................................. 326

Design, Verification and Documentation of Concurrent Systems
E.P. Gribomont .............................................................................. 360

A Formal Method for Hard Real-Time Programming
M. Gordon ..................................................................................... 378

Constructing and Refining Modules in a Type Theory
S.N. Ahmed and J.M. Morris .......................................................... 411

The Varieties of Refinement
J. Jacob ......................................................................................... 441

Timed Process Algebra, Petri Nets and Event Refinement
D. Murphy ..................................................................................... 456

Author Index ................................................................................... 479