

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

New York University, NY, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Helen Treharne Steve King
Martin Henson Steve Schneider (Eds.)

ZB 2005: Formal Specification and Development in Z and B

4th International Conference of B and Z Users
Guildford, UK, April 13-15, 2005
Proceedings



Springer

Volume Editors

Helen Treharne
University of Surrey
School of Electronics and Physical Sciences
Guildford, Surrey GU2 7XH, UK
E-mail: H.Treharne@surrey.ac.uk

Steve King
University of York
Department of Computer Science
Heslington, York, YO10 5DD, UK
E-mail: king@cs.york.ac.uk

Martin Henson
University of Essex
Department of Computer Science
Wivenhow Park, Colchester, Essex, CO4 3SQ, UK
E-mail: hensm@essex.ac.uk

Steve Schneider
University of Surrey
School of Electronics and Physical Sciences
Guildford, Surrey GU2 7XH, UK
E-mail: S.Schneider@surrey.ac.uk

Library of Congress Control Number: 2005923295

CR Subject Classification (1998): D.2.1, D.2.2, D.2.4, F.3.1, F.4.2, F.4.3

ISSN	0302-9743
ISBN-10	3-540-25559-1 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-25559-8 Springer Berlin Heidelberg New York

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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springeronline.com

© Springer-Verlag Berlin Heidelberg 2005
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11415787 06/3142 5 4 3 2 1 0

Preface

These proceedings record the papers presented at the 4th International Conference of B and Z Users (ZB 2005), held in the city of Guildford in the south-east of England. This conference built on the success of the previous three conferences in this series, ZB 2000, held at the University of York in the UK, ZB 2002, held at the *Laboratoire Logiciels Systèmes Réseaux* within the *Institut d'Informatique et Mathématique Appliquées de Grenoble* (LSR-IMAG) in Grenoble, France, and ZB 2003, held in Turku in Finland hosted by Åbo Akademi University and the Turku Centre for Computer Science (TUCS). ZB 2005 was held at the University of Surrey, Guildford, UK, hosted by the Department of Computing. The University has always placed particular emphasis on the applicability of its research and its relationship with industrial partners. In this context it is building up its formal methods activity as an area of strategic importance, with the establishment of a new group within the Department of Computing, and also with its support for this conference.

B and Z are two important formal methods that share a common conceptual origin; they are leading approaches in industry and academia for the specification and development (using formal refinement) of computer-based systems. At ZB 2005 the B and Z communities met once again to hold a fourth joint conference that simultaneously incorporated the 15th International Z User Meeting and the 6th International Conference on the B Method. Although organized logistically as an integral event, editorial control of the joint conference remained vested in two separate but cooperating programme committees that respectively determined its B and Z content, but in a coordinated manner.

All the submitted papers in this proceedings were peer reviewed by at least three reviewers drawn from the B or Z committee depending on the subject matter of the paper. For the first time for a ZB conference, reviewing, discussion and selection of papers were undertaken entirely electronically, with no face-to-face PC meeting. After an initial selection by each committee, a joint meeting of the chairs took place to finalize the selections and the conference programme.

The conference featured a range of contributions by distinguished invited speakers drawn from both industry and academia. The invited speakers addressed significant recent industrial applications of formal methods, as well as important academic advances serving to enhance their potency and widen their applicability. Our invited speakers for ZB 2005 were drawn from the UK, Australia and France.

Cliff Jones is a Professor of Computing Science at the University of Newcastle, UK. His career has been spent in both industry and academia, where his interests have been at the interface between research and application. He was behind the creation of the influential Vienna Development Method (VDM), one of the better-known formal methods (alongside Z and B!), during his time at

IBM in the 1970s. His interest in formal methods has now widened to encompass other aspects of dependability. Carroll Morgan is Australian Professorial Fellow at the School of Computer Science and Engineering, University of New South Wales, Australia. He has worked on Z, CSP, the refinement calculus, and probabilistic logic. He is the author of the seminal book on the refinement calculus ‘Programming from Specifications,’ and more recently (with Annabelle McIver) of ‘Abstraction, Refinement and Proof for Probabilistic Systems.’ His invited talk was sponsored by FME. Frédéric Badeau has been working on the B Method since 1994, and was part of the team that became ClearSy in 2001. He was involved in the development of the Atelier B tool, and has also worked on the B language. He has participated in a number of B software industrial projects within the railway industry. He has also been involved in some Event B projects in a research and development context. It was a pleasure to have three such eminent invited speakers at ZB 2005.

Besides its formal sessions the conference included tool demonstrations, exhibitions, a doctoral student poster session and tutorials. In particular, a Workshop on *Refinement* (REFINE 2005) was held on 12th April 2005, supported by the EPSRC RefineNet network, in association with the ZB 2005 meeting. In addition, the International B Conference Steering Committee (APCB) and the Z User Group (ZUG) used the conference as a convenient venue for open meetings intended for those interested in the B and Z communities respectively.

In one respect, the ZB 2005 meeting marked the end of an era, with the absence of a familiar face. Professor Jonathan Bowen, of London South Bank University, had been heavily involved in all three of the previous ZB conferences, and, prior to that, with Z User Group meetings since the first meetings in Oxford in the late 1980s. His contribution to the popularization of Formal Methods has been immense, both in conference organization and in his oft-cited website devoted to the subject. Both the Z and B communities are very grateful to him for his work, which continues in his activities with ZUG and with the BCS FACS group.

The topics of interest to the conference included: industrial applications and case studies using Z or using B; integration of model-based specification methods in the software development lifecycle; derivation of hardware-software architecture from model-based specifications; expressing and validating requirements through formal models; theoretical issues in formal development (e.g., issues in refinement, proof process, or proof validation, etc.); software testing versus proof-oriented development; tools supporting tools for the Z notation and the B Method; development by composition of specifications; validation of assembly of COTS by model-based specification methods; Z and B extensions and/or standardization.

The ZB 2005 conference was jointly initiated by the Z User Group (ZUG) and the International B Conference Steering Committee (APCB). The University of Surrey Computer Science Department provided all local organization, and financial backing was provided by ZUG. Without the great support from local staff at the University of Surrey and Royal Holloway, University of Lon-

don, ZB 2005 would not have been possible. In particular, much of the local organization was undertaken by Helen Treharne, with the assistance of Sophie Gautier-O'Shea, Neil Evans and Rob Delicata. ZB 2005 was sponsored by the Atomic Weapons Establishment (AWE), BCS-FACS (the British Computer Society Formal Aspects of Computing Science specialist group), BCS Guildford Branch, FME (Formal Methods Europe), the University of Surrey, Royal Holloway, University of London, and ZUG (Z User Group). BCS-FACS specifically sponsored prizes for best papers at the conference, and AWE sponsored students to attend the poster session. We are grateful to all those who contributed to the success of the conference.

Online information concerning the conference is available under the following Uniform Resource Locator (URL): <http://www.zb2005.org/>
This also provides links to further online resources concerning the B Method and Z notation.

We hope that all participants and other interested readers benefit scientifically from these proceedings and also find it stimulating in the process.

February 2005

Helen Treharne
Steve King
Martin Henson
Steve Schneider

Organization

Programme and Organizing Committees

The following people were members of the ZB 2005 Z Programme Committee and reviewed papers for the conference:

Co-chair: Martin Henson, University of Essex, UK

Co-chair: Steve King, University of York, UK

Keijiro Araki, Kyushu University, Japan

Rob Arthan, Lemma 1, Reading, UK

Jonathan Bowen, London South Bank University, UK

Neville Dean, Anglia Polytechnic University, UK

John Derrick, University of Sheffield, UK

Jin Song Dong, National University of Singapore

Mark d'Inverno, University of Westminster, UK

Wolfgang Grieskamp, Microsoft Research, USA

Ian Hayes, University of Queensland, Australia

Rob Hierons, Brunel University, UK

Jonathan Jacky, University of Washington, USA

Randolph Johnson, National Security Agency, USA

Kevin Lano, King's College London, UK

Yves Ledru, LSR-IMAG, Grenoble, France

Andrew Martin, Oxford University, UK

Fiona Polack, University of York, UK

Steve Reeves, University of Waikato, New Zealand

Mark Saaltink, ORA, Ottawa, Canada

Thomas Santen, Technical University of Berlin, Germany

Graeme Smith, University of Queensland, Australia

Susan Stepney, University of York, UK

Ian Toyn, University of York, UK

Mark Utting, University of Waikato, New Zealand

Sam Valentine, York, UK

The following served on the ZB 2005 B Programme Committee and reviewed papers for the conference:

Conference Chair: Steve Schneider, University of Surrey, UK

Chair: Helen Treharne, University of Surrey, UK

Richard Banach, University of Manchester, UK

Juan Bicarregui, CLRC, Oxfordshire, UK

Dominique Cansell, LORIA, University of Metz, France

Daniel Dolle, Siemens Transportation Systems, France
 Steve Dunne, University of Teesside, UK
 Mamoun Filali, CNRS, IRIT, Toulouse, France
 Marc Frappier, Université de Sherbrooke, Canada
 Andy Galloway, University of York, UK
 Henri Habrias, LINA, Université de Nantes, France
 Adrian Hilton, Praxis Critical Systems, UK
 Jacques Julliand, Université de Franche-Comté, Besançon, France
 Régine Laleau, LACL, IUT Fontainebleau, France
 Annabelle McIver, Macquarie University, Sydney, Australia
 Luis-Fernando Mejia, Alstom Transport Information Solutions, France
 Mike Poppleton, University of Southampton, UK
 Marie-Laure Potet, LSR-IMAG, Grenoble, France
 Ken Robinson, University of New South Wales, Australia
 Emil Sekerinski, McMaster University, Canada
 Véronique Vigié Donzeau-Gouge, CNAM, Paris, France
 Marina Waldén, Åbo Akademi University, Finland

The following people helped particularly with the organization of the conference in various capacities:

Conference Chair:	Steve Schneider, University of Surrey
Local Committee Chair:	Helen Treharne, University of Surrey
B Submissions:	Helen Treharne, University of Surrey
Z Submissions:	Martin Henson, University of Essex
Tools:	James Heather, University of Surrey
Posters:	Neil Evans, University of Surrey
Tutorials:	Ken Robinson, University of New South Wales
Proceedings:	Steve King, University of York
Local Arrangements:	Sophie Gautier-O'Shea & Neil Evans, University of Surrey
Website & CyberChair:	Rob Delicata, University of Surrey

We are especially grateful to the above for their efforts in ensuring the success of the conference.

External Referees

We are grateful to the following people who aided the programme committees in the reviewing of papers, providing additional specialist expertise:

Pascal André, University of Yamoussoukro, Ivory Coast
 Christian Attiogbé, University of Nantes, France
 Françoise Bellegarde, Université de Franche-Comté, Besançon, France
 Didier Bert, LSR-IMAG, Grenoble, France
 Jean-Paul Boidevex, IRIT, Toulouse, France
 Pontus Boström, Åbo Akademi University, Finland
 Michael Butler, University of Southampton, UK
 Orieta Celiku, Åbo Akademi University, Finland
 Frederic Gervais, CEDRIC (CNAM-IIE), GRIL, Université de Sherbrooke, Canada
 Alain Giorgetti, Université de Franche-Comté, Besançon, France
 Andy Gravell, University of Southampton, UK
 Maritta Heisel, University of Magdeburg, Germany
 Thai Son Hoang, University of New South Wales, Australia
 Olga Kouchnarenko, INRIA Lorraine, Nancy, France
 Michael Leuschel, University of Southampton, UK
 Yuan Fang Li, National University of Singapore
 Brian Matthews, CLRC, Oxfordshire, UK
 Dominique Méry, LORIA, Université Henri Poincaré, France
 Stephan Merz, INRIA Lorraine, Nancy, France
 Jean François Rolland, IRIT, Toulouse, France
 Marianne Simonot, CNAM, Paris, France
 Bill Stoddart, University of Teesside, UK
 David Streader, University of Waikato, New Zealand
 Jun Sun, National University of Singapore
 Raymond Turner, University of Essex, UK
 Guy Vidal-Naquet, Supélec, Gif, France
 Norbert Volker, University of Essex, UK
 Frank Zeyda, University of Teesside, UK

Support

ZB 2005 greatly benefited from the support of the following organizations

The University of Surrey
Royal Holloway, University of London

and sponsorship from

AWE
BCS-FACS
BCS Guildford Branch
FME
The University of Surrey
Royal Holloway, University of London
Z User Group

Tutorial Programme

The following tutorials were scheduled on the day before the main conference (April 12, 2005):

Expectation-Based Reasoning for Sequential Probabilistic Programs
Carroll Morgan, University of New South Wales, Australia

ProB: A Verification and Validation Tool for the B Method
Michael Leuschel, Michael Butler and Stephane Lo Presti, University of Southampton, UK

Case Study of a Complete Reactive System in Event-B: A Mechanical Press Controller
Jean-Raymond Abrial, ETH Zurich, Switzerland

Developing Z Tools with CZT
Mark Utting and Petra Malik, University of Waikato, New Zealand

Model-Based Testing Using Formal Models from Theory to Industrial Applications
Bruno Legeard and Mark Utting, University of Waikato, New Zealand

Table of Contents

Specification Before Satisfaction: The Case for Research into Obtaining the Right Specification (Extended Abstract) <i>Cliff B. Jones</i>	1
Visualising Larger State Spaces in PROB <i>Michael Leuschel, Edd Turner</i>	6
Non-atomic Refinement in Z and CSP <i>John Derrick, Heike Wehrheim</i>	24
Process Refinement in B <i>Steve Dunne, Stacey Conroy</i>	45
CZT: A Framework for Z Tools <i>Petra Malik, Mark Utting</i>	65
Model Checking Z Specifications Using SAL <i>Graeme Smith, Luke Wildman</i>	85
Proving Properties of Stateflow Models Using ISO Standard Z and CADiZ <i>Ian Toyn, Andy Galloway</i>	104
A Stepwise Development of the Peterson's Mutual Exclusion Algorithm Using B Abstract Systems <i>J. Christian Attiogbé</i>	124
An Extension of Event B for Developing Grid Systems <i>Pontus Boström, Marina Waldén</i>	142
The Challenge of Probabilistic <i>Event B</i> (Extended Abstract) <i>Carroll Morgan, Thai Son Hoang, Jean-Raymond Abrial</i>	162
Requirements as Conjectures: Intuitive DVD Menu Navigation <i>Jemima Rossmorris, Susan Stepney</i>	172
A Prospective-Value Semantics for the GSL <i>Frank Zeyda, Bill Stoddart, Steve Dunne</i>	187
Retrenchment and the B-Toolkit <i>Richard Banach, Simon Fraser</i>	203

Refinement and Reachability in Event_B	
<i>Jean-Raymond Abrial, Dominique Cansell, Dominique Méry</i>	222
A Rigorous Foundation for Pattern-Based Design Models	
<i>Soon-Kyeong Kim, David Carrington</i>	242
An Object-Oriented Structuring for Z Based on Views	
<i>Nuno Amálio, Fiona Polack, Susan Stepney</i>	262
Component Reuse in B Using ACL2	
<i>Yann Zimmermann, Diana Toma</i>	279
GeneSyst: A Tool to Reason About Behavioral Aspects of B Event Specifications. Application to Security Properties	
<i>Didier Bert, Marie-Laure Potet, Nicolas Stouls</i>	299
Formal Verification of a Type Flaw Attack on a Security Protocol Using Object-Z	
<i>Benjamin W. Long</i>	319
Using B as a High Level Programming Language in an Industrial Project: Roissy VAL	
<i>Frédéric Badeau, Arnaud Amelot</i>	334
Development via Refinement in Probabilistic B — Foundation and Case Study	
<i>Thai Son Hoang, Zhendong Jin, Ken Robinson, Annabelle McIver, Carroll Morgan</i>	355
Formal Program Development with Approximations	
<i>Eerke A. Boiten, John Derrick</i>	374
Practical Data Refinement for the Z Schema Calculus	
<i>Lindsay Groves</i>	393
Slicing Object-Z Specifications for Verification	
<i>Ingo Brückner, Heike Wehrheim</i>	414
Checking JML Specifications with B Machines	
<i>Fabrice Bouquet, Frédéric Dadeau, Julien Gros Lambert</i>	434
Including Design Guidelines in the Formal Specification of Interfaces in Z	
<i>Judy Bowen, Steve Reeves</i>	454

Some Guidelines for Formal Development of Web-Based Applications in B-Method	
<i>Abdolbaghi Rezazadeh, Michael Butler</i>	472
Author Index	493