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

LNCS 3455

ZB 2005: Formal Specification and Development in Z and B

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

Springer

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

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 Viguié 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*—

Cliff B. Jones

University of Newcastle upon Tyne,
Newcastle, NE1 7RU, UK
cliff.jones@ncl.ac.uk

Model-oriented specification techniques like VDM [Jon80, Jon90], Z [Hay93] and B [Abr96] have an enormous amount in common (cf. [Hay92, HJN94]). Among other things that this formal methods community shares is the view that one can start with a formal specification and show that a design/implementation satisfies that specification. It is however obvious that, if a specification does not actually reflect the real need, proving a program correct with respect to it is somewhat pointless.

As computers have become more powerful and less expensive, they have become ever more deeply embedded in the way nearly everyone works. In their short sixty year history, computers have moved from batch processors in their own buildings to work tools on every desk (or lap); essential components of administration,retail trade, banking and vehicles; and are on their way to becoming invisible dust sprinkled on who-knows-what. This, in itself, has changed the task of understanding the *requirements* of a system. Above all, the close interaction of people with computer systems makes it essential that designers consider the whole system when formulating a specification of the technical parts.

It is often easiest to make the point by looking at accidents. Donald MacKenzie in [Mac94, Mac01] has traced the cause of just over 1100 deaths where computer systems appear to be implicated (up to 1994). Three percent of the lives lost appear to be attributed to bugs! Far more common causes of accidents appear to be where humans misunderstand what is going on in a control system or the object being controlled. This is a much deeper issue than the details of an interface; in many cases it is a fundamental question of the allocation of tasks between person and machine. Key questions include the visibility of the state of the system being controlled and the extent to which operations the user can perform are clumped together.

Although accidents are shocking and thus grab attention, there is also a significant penalty in the deployment of systems which make their users' lives more difficult than they need be. The enormous cost of systems which are so unusable that they are not even deployed is reported weekly in newspapers.

Of course, we should use formal specification techniques and we still need research to make them more widely usable. But it would appear to be worthwhile to see whether there is also a *technical* response to the question of how one arrives at a specification which does reflect the needs of the environment in which

H. Treharne et al. (Eds.): ZB 2005, LNCS 3455, pp. 1–5, 2005.

a system will be embedded. Does the formal methods community have a contribution to make here? I believe so. Dines Bjørner's forthcoming books [Bjø05] tackle "domain modelling". This paper sets out some further research challenges to which we might be able to offer useful responses.

This invited talk will review some suggestions which have arisen in the six year "Interdisciplinary Research Collaboration on Dependability" (DIRC) — see the WWW pages at [WWW04] for details. DIRC is focusing its research on how to design *Dependable*[1] computer-based systems. The phrase "computer-based systems" is intended to emphasize that most computer systems today are deeply embedded into an environment which also involves people. For example, the requirement in a hospital is for dependability of the overall system. Sometimes, humans will use a computer system to achieve objectives even where they know that it delivers less than perfect information; on other occasions, computers can be programmed to warn when errors made by humans. People are less good than computers at narrowly specified repetitive tasks but are much better at recognising and reacting to exceptional situations. To achieve overall system dependability, both humans and programs must be properly deployed.

Some insights from the DIRC project include:

- An approach being worked on with Ian Hayes and Michael Jackson [HJJ03] looks at determining the specification of, say, a control system by first specifying a wider system including the phenomena of the physical world which are to be influenced. To avoid having to build a model of the behaviour of all physical components, assumptions about their behaviour are recorded using *rely conditions* (cf. [Jon83]). This leaves a clear record of assumptions which need to be considered before the control system is deployed. Development from the derived specification of the control system is conducted in the standard (formal) way.
- The design of boundaries that limit the *propagation of failures* is better articulated for technical systems than for the human part of computer-based systems. This is odd because the intuition about limiting, say, accounting errors by auditors is long established. Many examples can be cited to suggest that most human systems are "debugged" rather than designed. The motivation for where to place containment boundaries ought come from an analysis of the frequency of minor faults and the the danger of their affecting a wider system. This analysis ought precede the allocation of tasks to computers which, in turn of course, must be done prior to their specifications being frozen.
- A major cause of near or actual accidents is a "cognitive mismatch"[2] between an operator's view of what is going on and the actual state of affairs in the

[1] The classic text on the terminology of dependability is [Lap92]; see also [Ran00]; an attempt to formalise the useful trichotomy between faults, errors and failures is given in [Jon03].

[2] Both of James Reason's books [Rea90, Rea97] look at relevant issues: the earlier reference looks at a division of the sort of errors that humans make; the second has insightful analyses of many system failures. Perrow in [Per99] talks of "Normal accidents".

system they are trying to control. This was a significant factor in the "Three Mile Island" reactor incident. John Rushby [Rus99] has looked at pilot errors on the MD-88: in simulators, they frequently breach the required altitude ceiling. Rushby's careful formal analysis builds a state model of the pilot's understanding of the system and explores its interaction with a model of the aircraft systems. It would be informative to compare this approach with rely conditions.

- The general way in which *processes* (or procedures) are used in the human parts of computer-based systems is interesting. If one contrasts a traditional car production line with the depiction in the film "Apollo-13" of the search for a solution to the need to improvise CO_2 scrubbers in the damaged capsule, one sees that processes both limit action and reduce the need for information. Designing processes which cope with all exceptions is in many cases impossible and one argument for relying on humans in computer-based systems is precisely that they notice when it is safer to violate a procedure than to slavishly follow one that does not cover an exceptional case. Clearly, either following an inappropriate process or deviating from a correct process can both lead to system failure. But it is absolutely mandatory that thought is given to processes in the design of a computer-based system. Interestingly, one can spot errors in legislation where an algorithmic rule is frozen into law: there have been several cases in financial legislation where a well-intentioned trigger has had (or nearly had) counter-productive effects.
- Within DIRC, the role of *advisory systems* has received particular attention: [SPA03] studies an image analysis prompter used in the analysis of mammograms. Surprising conclusions include statistically significant evidence that under the tested conditions the most accurate operators can offer less accurate conclusions with the help of the advisory system than without its use. It is clear that the role of such advisory systems has to be considered far more widely than just by looking at their technical specifications. In fact, even pure safety limiters (where one would believe they can only increase safety) have been used by operators in a way which supplants their normal judgment.
- Systems can create other things whose dependability is the goal. In the simplest case, a production line might manufacture silicon chips and faults in the manufacturing process might result in faulty components for computers. A software example is a compiler that, if faulty, could translate a perfect program into machine code which does not respect the formal semantics of the source language. In many cases, the creation process is human and, for example, a designer of a bridge which fails to withstand expected forces is at fault. The creation of computer software is just such a process and is not always fault free! DIRC has provided an opportunity to look at Gerry Weinberg's conjectures in [Wei71] that different psychological types might be more or less adept at different sub-tasks within the broad area known as programming. The implications of this research for building dependable systems might include steering people toward the tasks at which they are likely to perform best (and probably be most content).

- If the above list were not daunting enough (and it is far from complete even with respect to DIRC's findings) there is another overriding concern. The sort of computer-based system we have been studying will always *evolve*. Designing a system which can be modified in reaction to a reasonable class of evolutions in the environment is extremely challenging. One class of system which has been studied within the DIRC project is *generic systems*. The justification of this sort of system is that it can be instantiated for a range of applications: characterising this range is itself a technical problem. It is clear that issues around evolution will have a long-term impact on dependability. There are related questions of how data survives such evolution which are equally challenging.

DIRC has identified far more than the above set of issues; the selection here has been based on the ease with which this one member of a project (involving more than fifty researchers) could pull together the information.

One key experience from the first three quarters of the project is the invaluable role of interdisciplinarity. Looking at experiments on psychological type and debugging performance required wholehearted collaboration of psychologists and computer scientists; tackling the mammography advisory system involved interaction between statisticians, sociologists and psychologists. DIRC could list many more examples of how our combination of psychologists, statisticians, sociologists and computer scientists has made real progress that no one of these disciplines could have accomplished.

My own disposition is to seek technical approaches to problems and I hope that the list above indicates that this is a viable challenge. But the DIRC project has been a superb example of collaboration and if faced with a complex application area, I would now know how to call on the expertise of other disciplines. In particular, the painstaking gathering of observational data needs sociologists.

We have learned two general things in the DIRC project which are worth passing on to others who might wish to follow such a wide interdisciplinary approach. Collaboration has to be based on respect for the disciplines of other researchers: values differ and publication strategies vary between disciplines but if it is good research by the standards of the other discipline one should not –for example– argue that it is not presented in the style of one's own discipline. The other message is to tackle application problems together as a team. With an "operations Research" (OR) like team representing several disciplines terminology problems disappear, contributions become understood and something is achieved which no single discipline could have envisaged.

Acknowledgments

My research acknowledgment is to the many colleagues involved in DIRC; it is a privilege to lead such an exciting project.

We are all grateful to EPSRC for the six year funding window which we feel was essential to foster such a wide interdisciplinary span.