Lecture Notes in Computer Science 5238

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
Alfred Kobsa
   University of California, Irvine, CA, 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
   University of California, Los Angeles, CA, USA
Doug Tygar
   University of California, Berkeley, CA, USA
Gerhard Weikum
   Max-Planck Institute of Computer Science, Saarbruecken, Germany
Preface

The ABZ 2008 conference was held in London during September 16–18, 2008. The conference aimed at contributing to the cross-fertilization of three rigorous methods that share a common conceptual foundation and are widely used in both academia and industry for the design and analysis of hardware and software systems, namely, abstract state machines, B, and Z. It followed on from the Dagstuhl seminar on Rigorous Methods for Software Construction and Analysis, which was organized in May 2006 by Jean-Raymond Abrial (ETH Zürich, Switzerland) and Uwe Glässer (Simon Fraser University – Burnaby, Canada), and brought together researchers from the ASM and the B community (see: http://www.dagstuhl.de/06191).

The conference simultaneously incorporated the 15th International ASM Workshop, the 17th International Conference of Z Users and the 8th International Conference on the B Method, which were present with separate Program Committees to select the papers published in separate tracks (see Chapters 2–4 of these proceedings). The conference covered a wide range of research spanning from theoretical and methodological foundations to tool support and practical applications. It was split into three main parts:

- A one-day common program of four invited lectures, see Chap. 1 of these proceedings, and the presentation of three papers selected among the submitted contributions
- Two days of contributed research papers and short presentations of work in progress, of industrial experience reports and of tool demonstrations, as documented in Chap. 2–5 of these proceedings
- Two tutorials on the ASM and B simulator tools CoreAsm and Pro-B

The conference was preceded by a UK EPSRC-funded Verified Software Repository Network (VSR-net) workshop on Monday, September 15, organized by Jim Woodcock and Paul Boca. This is reported in Chap. 6 of these proceedings, which includes an invited talk by Cliff Jones along with an overview of other technical talks at the VSR-net workshop covering progress on verification challenges.

We wish to thank the members of the three Program Committees and the numerous reviewers for their work, Springer for publishing the proceedings, and the sponsors for substantial financial support. In particular, the British Computer Society hosted the conference at their offices in central London, through the support of the BCS-FACS Specialist Group on Formal Aspects of Computing Science. Formal Methods Europe sponsored Wolfram Buettner’s attendance, Nokia provided welcome financial sponsorship and two devices which were awarded as best-paper prizes, and Praxis High Integrity Systems sponsored the conference bags. The EPSRC VSR-net Network enabled the VSR-net workshop
to be held free for attendees. London South Bank University provided access to the Union Jack Club for convenient accommodation for conference delegates. The Easychair system was used for management of the submission and reviewing process.

Further information on the ABZ2008 conference may be found online at: http://www.abz2008.org

Egon Börger
Michael Butler
Jonathan P. Bowen
Paul Boca
Organization

Program Chairs

Paul Boca  
Egon Börger  
Jonathan P. Bowen  
Michael Butler

Local Organization

Paul Boca

ASM Program Committee

Egon Börger (Chair)  
Alessandra Cavarra  
Andreas Friesen  
Uwe Glaesser  
Susanne Graf  
Kristina Lundqvist  
Andreas Prinz  
Elvinia Riccobene  
Klaus-Dieter Schewe  
Anatol Slissenko  
Jan Van den Bussche  
Margus Veanes  
Charles Wallace

B Program Committee

Christian Attiogbé  
Richard Banach  
Juan Bicarregui  
Michael Butler (Chair)  
Dominique Cansell  
Daniel Dolle  
Marc Frappier  
Jacques Julliand  
Regine Laleau  
Michael Leuschel  
Annabelle McIver
VIII Organization

Dominique Mery
Louis Mussat
Marie-Laure Potet
Ken Robinson
Steve Schneider
Emil Sekerinski
Bill Stoddart
Elena Troubitsyna
Mark Utting

Z Program Committee

Jonathan P. Bowen (Chair)
John Derrick
Leo Freitas
Martin Henson
Mike Hinchey
Randolph Johnson
Yves Ledru
Steve Reeves
Mark Utting
Sergiy Vilkomir
Jim Woodcock

VSR Day Organizers

Paul Boca
Jim Woodcock (Chair)

External Reviewers

Roozbeh Farahbod
Frederic Gervais
Stefan Hallerstede
Thai Son Hoang
Angel Robert Lynas
Hassan Mountassir
Martin Ouimet
Abdolbaghi Rezazadeh
Patrizia Scandurra
Laurent Voisin
# Table of Contents

## Chapter 1. ABZ Invited Talks

Complex Hardware Modules Can Now be Made Free of Functional Errors without Sacrificing Productivity ............................ 1

*Wolfram Büttnert*

The High Road to Formal Validation: Model Checking High-Level Versus Low-Level Specifications ............................. 4

*Michael Leuschel*

Modeling Workflows, Interaction Patterns, Web Services and Business Processes: The ASM-Based Approach .......................... 24

*Egon Börger and Bernhard Thalheim*

Refinement of State-Based Systems: ASMs and Big Commuting Diagrams (Abstract) .................................................. 39

*Gerhard Schellhorn*

## Chapter 2. ASM Papers

Model Based Refinement and the Tools of Tomorrow ...................... 42

*Richard Banach*

A Concept-Driven Construction of the Mondex Protocol Using Three Refinements .......................................................... 57

*Gerhard Schellhorn and Richard Banach*

A Scenario-Based Validation Language for ASMs .......................... 71

*Alessandro Carioni, Angelo Gargantini, Elvinia Riccobene, and Patrizia Scandurra*

Data Flow Analysis and Testing of Abstract State Machines ............. 85

*Alessandra Cavarra*

A Verified AsmL Implementation of Belief Revision .......................... 98

*Christoph Beierle and Gabriele Kern-Isberner*

Direct Support for Model Checking Abstract State Machines by Utilizing Simulation ..................................................... 112

*Jörg Beckers, Daniel Klünder, Stefan Kowalewski, and Bastian Schlich*

## Chapter 3. B Papers

On the Purpose of Event-B Proof Obligations .............................. 125

*Stefan Hallerstede*
Generating Tests from B Specifications and Test Purposes
Jacques Julliand, Pierre-Alain Masson, and Régis Tissot

Combining Scenario- and Model-Based Testing to Ensure POSIX
Compliance
Frédéric Dadeau, Adrien De Kermadec, and Régis Tissot

UseCase-Wise Development: Retrenchment for Event-B
Richard Banach

Towards Modelling Obligations in Event-B
Juan Bicarregui, Alvaro Arenas, Benjamin Aziz,
Philippe Massonnet, and Christophe Ponsard

A Practical Single Refinement Method for B
Steve Dunne and Stacey Conroy

The Composition of Event-B Models
Michael Poppleton

Reconciling Axiomatic and Model-Based Specifications Reprised
Ken Robinson

A Verifiable Conformance Relationship between Smart Card Applets
and B Security Models
Frédéric Dadeau, Julien Lamboley, Thierry Moutet, and
Marie-Laure Potet

Modelling Attacker’s Knowledge for Cascade Cryptographic
Protocols
Nazim Benaïssa

Using EventB to Create a Virtual Machine Instruction Set
Architecture
Stephen Wright

Chapter 4. Z Papers

Z2SAL - Building a Model Checker for Z
John Derrick, Siobhán North, and Anthony J.H. Simons

Formal Modeling and Analysis of a Flash Filesystem in Alloy
Eunsuk Kang and Daniel Jackson

Unit Testing of Z Specifications
Mark Utting and Petra Malik

Autonomous Objects and Bottom-Up Composition in ZOO Applied to
a Case Study of Biological Reactivity
Nuno Amálio, Fiona Polack, and Jing Zhang
Chapter 5. ABZ Short Papers

Integrating Z into Large Projects: Tools and Techniques ................. 337
  Anthony Hall

A First Attempt to Express KAOS Refinement Patterns with Event B ......................... 338
  Abderrahman Matoussi, Frédéric Gervais, and Régine Laleau

Verification and Validation of Web Service Composition Using Event B Method .......................................................... 339
  Idir Ait-Sadoune and Yamine Ait-Amour

Stability of Real-Time Abstract State Machines under Desynchronization ................................................. 341
  Joelle Cohen and Anatol Slissenko

XML Database Transformations with Tree Updates .................. 342
  Qing Wang, Klaus-Dieter Schewe, and Bernhard Thalheim

Dynamic Resource Configuration & Management for Distributed Information Fusion in Maritime Surveillance.................. 343
  Roozbeh Farahbod and Uwe Glässer

UML-B: A Plug-in for the Event-B Tool Set .......................... 344
  Colin Snook and Michael Butler

BART: A Tool for Automatic Refinement ............................... 345
  Antoine Requet

Model Checking Event-B by Encoding into Alloy
(Extended Abstract) ......................................................... 346
  Paulo J. Matos and João Marques-Silva

A Roadmap for the Rodin Toolset ........................................ 347
  Jean-Raymond Abrial, Michael Butler, Stefan Hallerstede, and Laurent Voisin

Exploiting the ASM Method for Validation & Verification of Embedded Systems ................................................. 348
  Angelo Gargantini, Elvinia Riccobene, and Patrizia Scandurra

Tool Support for the Circus Refinement Calculus .................... 349
  Alessandro Cavalcante Gurgel, Cristiano Gurgel de Castro, and Marcel Vinicius Medeiros Oliveira

Separation of Z Operations .............................................. 350
  Ramsay Taylor
# Table of Contents

BSmart: A Tool for the Development of Java Card Applications with the B Method ....................................................... 351  
*David Déharbe, Bruno Gomes, and Anamaria Moreira*

From ABZ to Cryptography (Abstract) ............................................. 353  
*Eerke A. Boiten*

Using ASM to Achieve Executability within a Family of DSL ............ 354  
*Ileana Ober and Ali Abou Dib*

Using Satisfiability Modulo Theories to Analyze Abstract State Machines (Abstract) .............................................. 355  
*Margus Veanes and Ando Saabas*

Formal Verification of ASM Models Using TLA⁺ ............................ 356  
*Hocine El-Habib Daho and Djilali Benhamamouch*

DIR 41 Case Study: How Event-B Can Improve an Industrial System Specification .................................................... 357  
*Christophe Metayer and Mathieu Clabaut*

FDIR Architectures for Autonomous Spacecraft: Specification and Assessment with Event-B ........................................ 358  
*Jean-Charles Chaudemar, Charles Castel, and Christel Seguin*

Object Modelling in the SystemB Industrial Project ........................ 359  
*Helen Treharne, Edward Turner, Steve Schneider, and Neil Evans*

## Chapter 6. VSR Day

Splitting Atoms with Rely/Guarantee Conditions Coupled with Data Reification ....................................................... 360  
*Cliff B. Jones and Ken G. Pierce*

ABZ2008 VSR-Net Workshop .................................................. 378  
*Jim Woodcock and Paul Boca*

Author Index ............................................................................. 381