Lecture Notes in Computer Science 8477

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 Kittner
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
TU Dortmund University, Germany

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA

Gerhard Weikum
Max Planck Institute for Informatics, Saarbruecken, Germany
Preface


This year’s ABZ was marked by two major events. In addition to ASM, B, Z, Alloy and VDM, ABZ 2014 saw the introduction of TLA (Temporal Logic of Actions) as the 6th formal method covered by the scope of the conference. In order to emphasise the integration of TLA, Leslie Lamport was invited to be one of the keynote speakers. He agreed to give an invited talk entitled “TLA+ for Non-Dummies” the year he was distinguished by the Turing Award. Congratulations!

After the “Steam Boiler” case study raised 20 years ago, the second event highlighting the 4th ABZ conference was the introduction of a case study track. The aeronautic context offered by the Toulouse area pushed us to look for a case study issued from this domain. Frédéric Boniol and Virginie Wiels kindly and immediately accepted to propose a “landing gear system” to be modelled within proof and refinement state based methods in the scope of ABZ. A separate proceedings volume, also published by Springer Verlag, is dedicated to this case study.

ABZ 2014 received 81 submissions covering the whole formal methods in the scope of the conference: Alloy, ASM, B, TLA, VDM and Z. These papers ranged on a wide spectrum covering fundamental contributions, applications in industrial contexts, and tool developments and improvements. Each paper was reviewed by at least three reviewers and the Program Committee accepted 13 long papers and 19 short papers. Furthermore, 8 long and 3 short papers were accepted for the case study track published in another proceedings volume. This selection process led to an attractive scientific programme.

In addition to the invited talk of Leslie Lamport, ABZ 2014 invited two other speakers. Gerhard Schellhorn from the University of Augsburg, Germany gave a talk entitled “Development of a Verified Flash File System” centered towards the ASM formal method and Laurent Voisin from the Systerel company, France with a talk entitled “The Rodin Platform has turned ten” reporting the progress achieved within the Rodin platform supporting Event-B. We would like to thank the three invited speakers for their contributions to the success of ABZ 2014.

ABZ 2014 would not have succeeded without the deep investment and involvement of the Program Committee members and the external reviewers who contributed to review (more than 250 reviews) and select the best contributions. This event would not exist if authors and contributors did not submit their proposals. We address our thanks to every person, reviewer, author, Program
Committee member and Organization Committee member involved in the success of ABZ 2014.

The EasyChair system was set up for the management of ABZ 2014 supporting submission, review and volume preparation processes. It proved to be a powerful framework.

We wish to express our special thanks to Jean-Raymond Abrial, Frédéric Boniol, Egon Börger and Virginie Wiels for their valuable support.

Finally, ABZ 2014 received the support of several sponsors, among them Airbus, CNES, CNRS, CRITT Informatique, CS, ENSEEIHT Toulouse, FME, INP Toulouse, IRIT, Midi Pyrénées Region, ONERA, SCCH, University Paul Sabatier Toulouse. Many thanks for their support.

June 2014

Yamine Ait Ameur
Klaus-Dieter Schewe
Organization

Program Committee

Jean-Raymond Abrial Consultant, France
Yamine Ait Ameur IRIT/INPT-ENSEEIHT, France
Richard Banach University of Manchester, UK
Eerke Boiten University of Kent, UK
Frederic Boniol ONERA, France
Michael Butler University of Southampton, UK
Egon Börger University of Pisa, Italy
Ana Cavalcanti University of York, UK
David Deharbe Universidade Federal do Rio Grande do Norte, Brazil
John Derrick University of Sheffield, UK
Juergen Dingel Queen’s University, Canada
Kerstin Eder University of Bristol, UK
Roozbeh Farahbod SAP Research, Germany
Mamoun Filali-Amine IRIT-Toulouse, France
John Fitzgerald University of Sherbrooke, Canada
Vincenzo Gervasi University of Pisa, Italy
Dimitra Giannakopoulou NASA Ames, USA
Uwe Glässer Simon Fraser University, Canada
Stefania Gnesi ISTI-CNR, Italy
Lindsay Groves Victoria University of Wellington, New Zealand
Stefan Hallerstedt University of Düsseldorf, Germany
Klaus Havelund California Institute of Technology, USA
Ian J. Hayes University of Queensland, Australia
Rob Hierons Brunel University, UK
Thai Son Hoang Swiss Federal Institute of Technology Zurich, Switzerland
Sarfraz Khurshid The University of Texas at Austin, USA
Regine Laleau Paris Est Creteil University, France
Leslie Lamport Microsoft Research, USA
Peter Gorm Larsen Aarhus School of Engineering, Denmark
Thierry Lecomte Clearsy, France
Michael Leuschel University of Düsseldorf, Germany
Yuan-Fang Li Monash University, Australia
Zhiming Liu United Nations University - International Institute for Software Technology, Macao
Tiziana Margaria University of Potsdam, Germany
Atif Mashkoor Software Competence Center Hagenberg, Austria
Dominique Mery Université de Lorraine, LORIA, France
Stephan Merz Inria Lorraine, France
Mohamed Mosbah LaBRI - University of Bordeaux, France
Cesar Múñoz NASA Langley, USA
Uwe Nestmann Technische Universität Berlin, Germany
Chris Newcombe Amazon.com, USA
Jose Oliveira Universidade do Minho, Portugal
Luísa Petre Ábo Akademi University, Finland
Andreas Prinz University of Agder, Norway
Alexander Raschke Institute of Software Engineering and Compiler Construction, Germany
Elvinia Riccobene DTI - University of Milan, Italy
Ken Robinson The University of New South Wales, Australia
Thomas Rodeheffer Microsoft Research, USA
Alexander Romanovsky Newcastle University, UK
Thomas Santen European Microsoft Innovation Center in Aachen, Germany
Patrizia Scandurra DIIMM - University of Bergamo, Italy
Gerhard Schellhorn University of Augsburg, Germany
Klaus-Dieter Schewe Software Competence Center Hagenberg, Austria
Steve Schneider University of Surrey, UK
Colin Snook University of Southampton, UK
Jing Sun The University of Auckland, New Zealand
Mana Taghdiri KIT, Germany
Margus Veanes Microsoft Research, USA
Marcel Verhoef Chess, The Netherlands
Friedrich Vogt University of Technology Hamburg-Harburg, Germany
Laurent Voisin Systerel, France
Qing Wang Information Science Research Centre, New Zealand
Virginie Wiels ONERA, France
Kirsten Winter University of Queensland, Australia

Additional Reviewers

Arcaini, Paolo Couto, Luís Diogo
Attiogbe, Christian Cunha, Alcino
Barbosa, Haniel Ernst, Gidon
Coleman, Joey Esparza Isasa, José Antonio
Colvin, Robert Fantechi, Alessandro
Gervais, Frederic
Herbreteau, Frédéric
Iliasov, Alexei
Kossak, Felix
Ladenberger, Lukas
Leupolz, Johannes
Macedo, Nuno
Mammar, Amel
Nalbandyan, Narek
Neron, Pierre

Pfähler, Jörg
Sandvik, Petter
Senni, Valerio
Singh, Neeraj
Tarasyuk, Anton
Tounsi, Mohamed
Treharne, Helen
Winter, Kirsten
Yaghoubi Shahir, Hamed
Abstract. I will discuss the motivation underlying TLA+ and some of the language’s subtleties. Since Springer-Verlag requires a longer abstract, here is a simple sample TLA+ specification:

---

MODULE Euclid
(* This module specifies a version of Euclid’s algorithm *)
(* for computing the greatest common divisor of two *)
(* positive integers. *)
EXTENDS Integers

CONSTANTS M, N

ASSUME /
  \ M \in Nat \ {0}
  \ N \in Nat \ {0}

VARIABLES x, y

Init == (x = M) \ (y = N)

Next ==
  ( x > y \
    \ x’ = x - y
    \ y’ = y )
  \ ( y > x \
    \ y’ = y - x
    \ x’ = x )

Spec == Init \ [\] [Next]_<x, y>
---
## Table of Contents

The Rodin Platform Has Turned Ten ................................................. 1  
*Laurent Voisin and Jean-Raymond Abrial*

Development of a Verified Flash File System ........................................... 9  
*Gerhard Schellhorn, Gidon Ernst, Jörg Pfähler, Dominik Haneberg, and Wolfgang Reif*

Why Amazon Chose TLA+ .......................................................... 25  
*Chris Newcombe*

Translating B to TLA+ for Validation with TLC ................................. 40  
*Dominik Hansen and Michael Leuschel*

αRby–An Embedding of Alloy in Ruby .............................................. 56  
*Aleksandar Milicevic, Ido Efrati, and Daniel Jackson*

MAZE: An Extension of Object-Z for Multi-Agent Systems ................. 72  
*Graeme Smith and Qin Li*

Quasi-Lexicographic Convergence .................................................. 86  
*Stefan Hallerstede*

Towards B as a High-Level Constraint Modelling Language: Solving the Jobs Puzzle Challenge .................................................. 101  
*Michael Leuschel and David Schneider*

Analysis of Self-* and P2P Systems Using Refinement ..................... 117  
*Manamiary Bruno Andriamiarina, Dominique Méry, and Neeraj Kumar Singh*

*B Formal Validation of ERTMS/ETCS Railway Operating Rules ..... 124  
*Rahma Ben Ayed, Simon Collart-Dutilleul, Philippe Bon, Akram Idani, and Yves Ledru*

Modelling Energy Consumption in Embedded Systems with VDM-RT .................................................. 130  
*José Antonio Esparza Isasa, Peter Würtz Vinther Jørgensen, Claus Ballegård Nielsen, and Stefan Hallerstede*

Sealed Containers in Z .............................................................. 136  
*Eerke Boiten and Jeremy Jacob*
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying Transaction Control to Serialize Concurrent Program</td>
<td>142</td>
</tr>
<tr>
<td>Egon Börger and Klaus-Dieter Schewe</td>
<td></td>
</tr>
<tr>
<td>Distributed Situation Analysis: A Formal Semantic Framework</td>
<td>158</td>
</tr>
<tr>
<td>Narek Nalbandyan, Uwe Glässer, Hamed Yaghoubi Shahir, and Hans Wehn</td>
<td></td>
</tr>
<tr>
<td>Introducing Aspect–Oriented Specification for Abstract State Machines</td>
<td>174</td>
</tr>
<tr>
<td>Marcel Dausend and Alexander Raschke</td>
<td></td>
</tr>
<tr>
<td>Modular Refinement for Submachines of ASMs</td>
<td>188</td>
</tr>
<tr>
<td>Gidon Ernst, Jörg Pfähler, Gerhard Schellhorn, and Wolfgang Reif</td>
<td></td>
</tr>
<tr>
<td>Towards ASM-Based Formal Specification of Self-Adaptive Systems</td>
<td>204</td>
</tr>
<tr>
<td>Elvinia Riccobene and Patrizia Scandurra</td>
<td></td>
</tr>
<tr>
<td>Distributed ASM - Pitfalls and Solutions</td>
<td>210</td>
</tr>
<tr>
<td>Andreas Prinz and Edel Sherratt</td>
<td></td>
</tr>
<tr>
<td>WebASM: An Abstract State Machine Execution Environment for the Web</td>
<td>216</td>
</tr>
<tr>
<td>Simone Zenzaro, Vincenzo Gervasi, and Jacopo Soldani</td>
<td></td>
</tr>
<tr>
<td>Formal System Modelling Using Abstract Data Types in Event-B</td>
<td>222</td>
</tr>
<tr>
<td>Andreas Fürst, Thai Son Hoang, David Basin, Naoto Sato, and Kunihiko Miyazaki</td>
<td></td>
</tr>
<tr>
<td>Formal Derivation of Distributed MapReduce</td>
<td>238</td>
</tr>
<tr>
<td>Inna Pereverzeva, Michael Butler, Asieh Salehi Fathabadi, Linas Laibinis, and Elena Troubitsyna</td>
<td></td>
</tr>
<tr>
<td>Validating the RBAC ANSI 2012 Standard Using B</td>
<td>255</td>
</tr>
<tr>
<td>Nghi Huynh, Marc Frappier, Amel Mammar, Régine Laleau, and Jules Desharnais</td>
<td></td>
</tr>
<tr>
<td>Invariant Guided System Decomposition</td>
<td>271</td>
</tr>
<tr>
<td>Richard Banach</td>
<td></td>
</tr>
<tr>
<td>Understanding and Planning Event-B Refinement through Primitive</td>
<td>277</td>
</tr>
<tr>
<td>Rationales</td>
<td></td>
</tr>
<tr>
<td>Tsutomu Kobayashi, Fuyuki Ishikawa, and Shinichi Honiden</td>
<td></td>
</tr>
<tr>
<td>Templates for Event-B Code Generation</td>
<td>284</td>
</tr>
<tr>
<td>Andrew Edmunds</td>
<td></td>
</tr>
<tr>
<td>The BWare Project: Building a Proof Platform for the Automated</td>
<td>290</td>
</tr>
<tr>
<td>Verification of B Proof Obligations</td>
<td></td>
</tr>
<tr>
<td>David Delahaye, Catherine Dubois, Claude Marché, and David Mentré</td>
<td></td>
</tr>
</tbody>
</table>
Tuning the Alt-Ergo SMT Solver for B Proof Obligations ................. 294
Sylvain Conchon and Mohamed Iguernelala

Fixed-Point Arithmetic Modeled in B Software Using Reals ............ 298
Jérôme Guéry, Olivier Rolland, and Joris Rehm

Bounded Model Checking of Temporal Formulas with Alloy ............ 303
Alcino Cunha

Formal Verification of OS Security Model with Alloy and Event-B ...... 309
Petr N. Devyanin, Alexey V. Khoroshilov, Victor V. Kuliamin,
Alexander K. Petrenko, and Ilya V. Shchepetkov

Detecting Network Policy Conflicts Using Alloy ....................... 314
Ferney A. Maldonado-Lopez, Jaime Chavarriaga, and Yezid Donoso

Staged Evaluation of Partial Instances in a Relational Model Finder . . . 318
Vajih Montaghami and Derek Rayside

Domain-Specific Visualization of Alloy Instances ...................... 324
Loïc Gammaitoni and Pierre Kelsen

Optimizing Alloy for Multi-objective Software Product Line
Configuration............................................................................. 328
Ed Zulkoski, Chris Kleynhans, Ming-Ho Yee, Derek Rayside, and
Krzysztof Czarnecki

Author Index ............................................................................. 335