Lecture Notes in Computer Science 2589

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

Egon Börger Angelo Gargantini
Elvinia Riccobene (Eds.)

Abstract State Machines 2003

Advances in Theory and Practice

10th International Workshop, ASM 2003
Taormina, Italy, March 3-7, 2003
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Egon Börger
Università di Pisa, Dipartimento di Informatica
Via Buonarotti 2, 56127 Pisa, Italy
E-mail: boerger@di.unipi.it

Angelo Gargantini
Università di Catania, CEA
Piazza Università 2, 95124 Catania, Italy
E-mail: gargantini@dmi.unict.it

Elvinia Riccobene
Università di Catania, Dipartimento di Matematica e Informatica
Città Universitaria, viale A. Doria 6, 95125 Catania, Italy
E-mail: riccobene@dmi.unict.it

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliographie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): F.3, D.2, F.4.1, D.3, H.2.3

ISSN 0302-9743
ISBN 3-540-00624-9 Springer-Verlag 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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

© Springer-Verlag Berlin Heidelberg 2003
Printed in Germany

Typesetting: Camera-ready by author, data conversion by DA-TeX Gerd Blumenstein
Printed on acid-free paper SPIN: 10872467 06/3142 5 4 3 2 1 0

ASM 2003—A Double Anniversary in Sicily

ASM 2003 and this volume constitute a double landmark in the short history of the Abstract State Machine method for the design and the analysis of complex software/hardware systems. The volume contains the Proceedings of the 10th *International Workshop on Abstract State Machines* (ASM 2003), held in Taormina (Sicily) from March 3rd to March 7th, 2003. The anniversary edition of this workshop was the first one held in Italy, the country where Yuri Gurevich, in his influential 1986 and 1990 Spring lectures in Pisa, explained for the first time his ideas about generalizing Turing's thesis by a resource-bound-aware model of computation[1], and the country where the first of an ever growing series of European Ph.D. and habilitation theses was written (1989–1992)[2] which apply ASMs to real-life computing systems or develop their theoretical foundation further. It was also 10 years ago, in Sicily, that the fundamental Lipari Guide[3] saw the light, namely at the Lipari Summer School which in 1993 was devoted to *Specification and Validation Methods*.

The previous editions of the international workshop series on Abstract State Machines were held in the following European cities: Dagstuhl, Germany (2002); Las Palmas de Gran Canaria, Spain (2001); Monte Verità, Switzerland (2000); Toulouse, France (1999); Magdeburg, Germany (1998); Cannes, France (1998, 1997); Paderborn, Germany (1996); and Hamburg, Germany (1994).

ASM 2003 aimed at enforcing two valuable traditions of ASM workshops. In the first place ASM 2003 was devoted to both the theory and the multiple real-life applications of ASMs, with the goal to provide a forum for a survey and a critical evaluation of the current academic and industrial developments of the ASM method, aiming at a fruitful interaction between theory and practice. As organizers we were eager to maintain at ASM 2003 the vivid, frank but fair style of scientific disputation which has characterized past editions of the workshop.

The second concern of ASM 2003 was to offer a moment of reflection upon the place the ASM method occupies in the field of Computer Science, paying attention in particular to the relation of the method to similar or complementary system development and analysis approaches. This was also one of the reasons why in the past half of the ASM workshops were held as part of larger computer science conferences: ASM 2001 as part of Eurocast'01, ASM 1999 as part of FME'99, ASM 1998 in Magdeburg as part of GI-Jahrestagung, and ASM 1994 as part of the IFIP World Congress. The goal is to pave the way for an integration of

[1] For historical details see: E. Börger, The origins and the development of the ASM method for high level system design and analysis, *J. of Universal Computer Science*, 8(1):2–74, 2002.

[2] E. Riccobene, *Modelli Matematici per Linguaggi Logici*, Ph.D. thesis, University of Catania, Academic year 1991/92.

[3] Y. Gurevich, Evolving Algebras 1993: Lipari Guide, In E. Börger, editor, *Specification and Validation Methods*, pages 9–36. Oxford University Press, 1995.

ASM-based modeling, validation and verification techniques into current system engineering methods, truly enriching them (certainly not only rephrasing them in ASM terms), and to identify new challenges for the ASM method.

In fact the invited lectures of ASM 2003 covered not only internal progress and new frontiers for ASMs (lectures by Yuri Gurevich, Microsoft Research, Redmond, USA, and Egon Börger, University of Pisa, Italy), but also some areas of major challenges for new applications of the ASM method:

- object-oriented, component-based design and program verification techniques (lecture by Bertrand Meyer, ETH, Zürich, Switzerland),
- mobile computing (lecture by Gruia-Catalin Roman, Washington University in St. Louis, USA),
- testing (lectures by Antonia Bertolino, ISTI at the Italian Research Council, Pisa, Italy and Klaus Havelund, NASA Research Center, USA),
- concurrency techniques (lecture by Perdita Stevens, University of Edinburgh, UK),
- refinement techniques (lecture by John Derrick, University of Kent, Canterbury, UK).

The contributed *research papers* and *short presentations* of work in progress developed ASM applications and the theory further and contributed to the themes of the invited lectures. The reader will find modeling and analysis work for new kinds of systems (among others for knowledge management, information services, database systems, UML, abstract encryption, the new Java memory model, quantum algorithms), comparative studies of different methods and tools for system description (e.g., big-step and small-step semantics, expression evaluation principles in various programming languages, the MDG tool, ASMs as a platform for the analysis of distributed production control systems at multiple levels of abstraction), advances in the theory of ASMs (analysis of turbo ASMs, decidability problems, support for recursion) and in teaching ASMs, testing, model-checking, etc. In addition ASM 2003 featured industrial experience reports and tool demonstrations.

We thank Uwe Glässer (Simon Fraser University, Vancouver, Canada) and Anatol Slissenko (University 12, Paris, France) for having organized as part of ASM 2003 a round table discussion on the challenging theme of rigorous mathematical models of real time in distributed computing. We also thank the speakers of the round table: Ernst-Rüdiger Olderog (University of Oldenburg, Germany), Andreas Prinz (DResearch Digital Media Systems, Berlin, Germany), and Susanne Graf (Verimag, Grenoble, France). As formulated by Uwe Glässer and Anatol Slissenko, the round table on time in specifications discussed some vision of the following and related topics:

- What are the types of timed systems to consider? What are time constraints and operations over time that arise in practice?
- How are timed systems specified and implemented in practice and what kind of specification languages are demanded or desired by practical specifications?

- How is time represented in existing specification languages? What are the domains of application of these languages and what timed systems are outside these domains?
- Continuous versus discrete time: what are the practical and theoretical advantages or disadvantages of using these models of time?
- What are the theoretical problems in defining the semantics of timed systems?
- How should we represent and simulate time in ASM and ASML?

We thank our colleagues in the program committee and the additional reviewers for their support in evaluating the papers submitted to ASM 2003. We thank Jim Huggins for having placed a copy of the extended abstracts of the work in progress on the ASM website in Michigan. We thank Springer-Verlag, and in particular Alfred Hofmann, for having accepted these proceedings for the LNCS series. We thank our colleagues and students in the University of Catania for their generous help with the organization of ASM 2003. For financial support of the workshop we thank our universities and Microsoft Research. Last, but not least, we thank the participants of ASM 2003 for having made our work useful.

November 2002

Egon Börger
Angelo Gargantini
Elvinia Riccobene

Organization Committee

Egon Börger	(University of Pisa, Italy)
Elvinia Riccobene	(University of Catania, Italy)

Program Committee

Richard Banach	(University of Manchester, UK)
Danièle Beauquier	(University of Paris 12, France)
Egon Börger	(University of Pisa, Italy) (Co-chair)
Jim Davies	(Oxford University, UK)
Gerard R. Renardel de Lavalette	(University of Groningen, The Netherlands)
Uwe Glässer	(Simon Fraser University, Canada)
Peter Päppinghaus	(Siemens, München, Germany)
Elvinia Riccobene	(University of Catania, Italy) (Co-chair)
Robert Stärk	(ETH Zürich, Switzerland)
Peter H. Schmitt	(Universität Karlsruhe, Germany)
Margus Veanes	(Microsoft Research, Redmond, USA)
Wolf Zimmermann	(Universität Halle-Wittenberg, Germany)

Local Committee

Angelo Gargantini	(University of Catania, Italy)
Elvinia Riccobene	(University of Catania, Italy)
Gimpaolo Bella	(University of Catania, Italy)

Additional Reviewers

I. Attali	A. Gargantini	W. Löwe
G. Bella	Y. Gurevich	M. Nicolosi Asmundo
A. Bertolino	W. Hesselink	P. Scandurra
Y. Bryukhov	J. Huggins	A. Slissenko
A. Cavarra	J. Jongejan	H. Wietze de Haan
W. Gabrisch	M. Kardos	

Sponsoring Institutions

University of Pisa, Italy
University of Catania, Italy
Microsoft Research, Redmond, WA, USA
Proteo S.p.A., Catania, Italy

Table of Contents

Invited Papers

Software Testing Research and Practice 1
Antonia Bertolino

Abstract State Processes 22
Tommaso Bolognesi and Egon Börger

Recent Advances in Refinement 33
John Derrick and Eerke Boiten

Partial Updates Exploration II 57
Yuri Gurevich and Nikolai Tillmann

Experiments with Test Case Generation and Runtime Analysis 87
Cyrille Artho, Doron Drusinksy, Allen Goldberg, Klaus Havelund, Mike Lowry, Corina Pasareanu, Grigore Roşu, and Willem Visser

A Framework for Proving Contract-Equipped Classes 108
Bertrand Meyer

Mobile UNITY Schemas for Agent Coordination 126
Gruia-Catalin Roman and Jamie Payton

UML and Concurrency 151
Perdita Stevens

Research Papers

A Unified Formal Specification and Analysis of the New Java Memory Models 166
Varsha Awhad and Charles Wallace

Modelling Conditional Knowledge Discovery and Belief Revision by Abstract State Machines 186
Christoph Beierle and Gabriele Kern-Isberner

Formal Description of a Distributed Location Service for Mobile Ad Hoc Networks 204
András Benczúr, Uwe Glässer, and Tamás Lukovszki

Remarks on Turbo ASMs for Functional Equations and Recursion Schemes 218
Egon Börger and Tommaso Bolognesi

Integrating UML Static and Dynamic Views and Formalizing the Interaction Mechanism of UML State Machines 229
Alessandra Cavarra, Elvinia Riccobene, and Patrizia Scandurra

The Hidden Computation Steps of Turbo Abstract State Machines 244
Nicu G. Fruja and Robert F. Stärk

Using Spin to Generate Tests from ASM Specifications 263
Angelo Gargantini, Elvinia Riccobene, and Salvatore Rinzivillo

Interfacing ASM with the MDG Tool 278
Amjad Gawanmeh, Sofiène Tahar, and Kirsten Winter

ASMs versus Natural Semantics: A Comparison with New Insights 293
Sabine Glesner

Quantum Computing and Abstract State Machines 309
Erich Grädel and Antje Nowack

Consistent Integration for Sequential Abstract State Machines 324
Marianna Nicolosi Asmundo and Elvinia Riccobene

Deciding the Verification Problem for Abstract State Machines 341
Antje Nowack

An ASM Semantics of UML Derived from the Meta-model and Incorporating Actions 356
Ileana Ober

Privacy, Abstract Encryption and Protocols: An ASM Model – Part I 372
Dean Rosenzweig, Davor Runje, and Neva Slani

A Framework for Modeling the Semantics of Expression Evaluation with Abstract State Machines 391
Wolf Zimmermann and Axel Dold

Extended Abstracts

Using AsmL for Runtime Verification 407
Mike Barnett, Wolfram Schulte, and Nikolai Tillmann

Modeling Information Services on the Basis of ASM Semantics 408
Aleksander Binemann-Zdanowicz and Bernhard Thalheim

Designing the Parlay Call-Control Using ASMs 411
Paolo Falcarin and Alessandra Cavarra

Test Case Generation from AsmL Specifications 413
Wolfgang Grieskamp, Lev Nachmanson, Nikolai Tillmann, and Margus Veanes

Teaching ASMs, Teaching with ASMs: Opportunities in Undergraduate Education 414
James Huggins, Jean Mayo, and Charles Wallace

Using ASM Specifications for Compiler Testing 415
Alexey Kalinov, Alexandre Kossatchev, Alexander Petrenko, Mikhail Posypkin, and Vladimir Shishkov

ASMs as Integration Platform towards Verification and Validation of Distributed Production Control Systems at Multiple Levels of Abstraction 416
Martin Kardos and Ulrich Nickel

AsmL Specification of a Ptolemy II Scheduler 417
Daniel Lázaro Cuadrado, Peter Koch, and Anders P. Ravn

ASM Specification of Database Systems 418
Andreas Prinz and Bernhard Thalheim

The Computable Kernel of ASM 421
Wolfgang Reisig

A Non-standard Approach to Operational Semantics for Timed Systems 423
Heinrich Rust

Parallelism versus Nondeterminism: On the Semantics of Abstract State Machines 425
Wolfram Schulte

Author Index 427