Lecture Notes in Computer Science 5115

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Jean-Raymond Abrial Uwe Glässer (Eds.)

Rigorous Methods for Software Construction and Analysis

Essays Dedicated to Egon Börger
on the Occasion of His 60th Birthday

Springer

Volume Editors

Jean-Raymond Abrial
Marseille, France
E-mail: jrabrial@neuf.fr

Uwe Glässer
Simon Fraser University
School of Computing Science
Burnaby, BC, Canada V5A 1S6
E-mail: glaesser@cs.sfu.ca

The illustration appearing on the cover of this book is the work of Daniel Rozenberg (DADARA).

Library of Congress Control Number: 2009942153

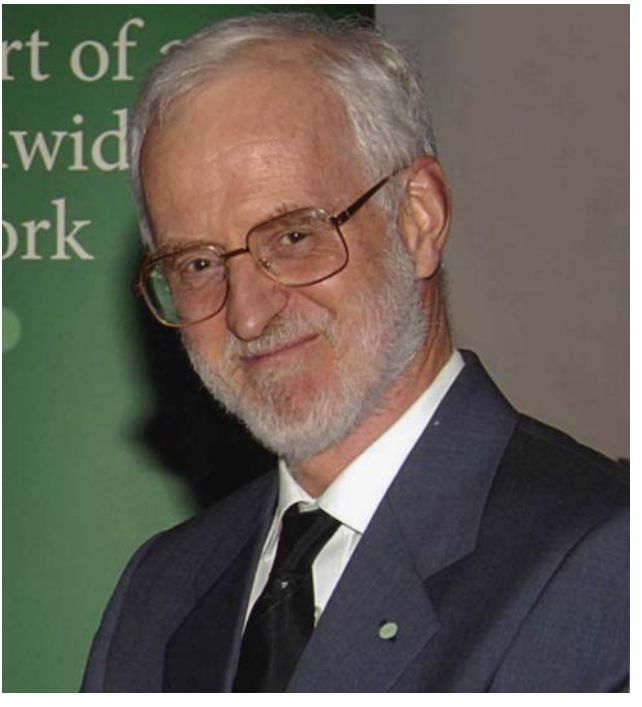
CR Subject Classification (1998): F.1, F.2.1-2, F.4.1, F.3, D.2.4, D.2-3, I.2.2

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-642-11446-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-11446-5 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12821952 06/3180 5 4 3 2 1 0

Preface



Egon Börger

Tribute to Egon Börger on the Occasion of his 60th Birthday

Jean-Raymond Abrial[1] and Uwe Glässer[2]

[1] jrabrial@neuf.fr
[2] glaesser@cs.sfu.ca

Egon Börger was born on May 13, 1946, in Westfalia (Germany). After the classic baccalauréat, from 1965-1971 he studied philosophy, logic and mathematics at the Sorbonne (Paris, France), Institut Supérieur de Philosophie de Louvain (Belgium), Université de Louvain and Universität Münster (Germany), where he got his doctoral degree and in 1976 his "Habilitation" in mathematics. The themes of his doctoral dissertation, *Reduction classes in Krom and Horn formulae*, and of his "Habilitationsschrift," *A simple method for determining the degree of unsolvability of decision problems for combinatorial systems*, have their root in the computational view of mathematical logic held at the time at the Institute for Logic and Foundations of Mathematics at the University of Münster, a tradition going back to (among others) Leibniz, Ackermann, Gödel, Post, Turing, Kleene, and associated in Münster with the names of the founder of the institute, Heinrich Scholz, and his followers Hans Hermes, Gisbert Hasenjäger and Dieter Rödding. This heritage determined the focus of Börger's logical investigations in what nowadays is called computability and computational complexity theory and his early interest in applying methods from logic to solve problems in computer science.

Thus, it does not come as a surprise that from 1972 to 1976 Börger followed Edoardo Caianello's call to help create the computer science department at the Università di Salerno (Italy), where he developed the curriculum for and taught the courses on Algorithms, Computational Complexity Theory, Semantics and Logic. After a short period (1976-1978) as Dozent of Mathematical Logic at the University of Münster, Börger became Professor for Theoretical Computer Science at the University of Dortmund (Germany), where he wrote his book on *Computability, Complexity, Logic* [1], which went through numerous editions, for over a decade became the main reference book for courses on the subject in German universities, and has been translated into English and Italian. Börger spent the academic year 1982–1983 as professor at the then new computer science department of the Università di Udine (Italy), and in 1985 accepted a computer science chair at the Università di Pisa (Italy), which he has held since then, rejecting various offers from other universities.

Through editing books and organizing workshops, summer schools, conferences, including various seminars at the Mathematical Research Institute in Oberwolfach and at Schloss Dagstuhl, Börger has been committed since the late 1970s to promoting a concrete interaction between logicians and computer

scientists, based upon his conviction that the major challenges for contemporary logic are to be found in applying logical methods in computer science. To provide an institutional basis for such an interaction, in 1986–1987 he founded together with his colleagues Michael Richter and Hans Kleine Büning the series of annual Computer Science Logic workshops. In their sixth edition, in San Miniato near Pisa, these meetings became the Annual Conference of the European Association for Computer Science Logic (http://www.eacsl.org/). The EACSL was founded on Börger's initiative on July 14, 1992, by 37 computer scientists and logicians from 14 countries gathered in a Dagstuhl Seminar on Computer Science Logic Börger had organized together with his colleagues Richter, Kleine Büning, and Yuri Gurevich. From 1992 to 1997 Börger acted as first EACSL President.

Börger's research activities in logic and complexity theory in the years 1969–1989 culminated in the book on *The Classical Decision Problem* [2], for which he wrote the first half, the one on the classification of undecidable classes of first-order logic formulae, co-authored by Erich Grädel who wrote the chapters on the complexity of the decidable classes, except for the section on the Shelah class that was written by Gurevich. The years 1986–1989 brought a shift of interest. They were characterized by a close cooperation between Börger and Gurevich on the eventual definition, by Gurevich in 1993 [3], of the notion of Abstract State Machines (ASMs)[1]. The idea grew out of Gurevich's foundational concern about sharpening Turing's thesis by a model of computation that explicitly recognizes the finiteness of computers, a theoretical effort that was crowned by success in 2000 when on the basis of three natural axioms Gurevich succeeded to prove that "Sequential Abstract State Machines capture sequential algorithms" [5].

Börger's interest was triggered by an attempt to use ASMs to model the logic programming language Prolog. During his sabbatical from 1989 to 1990, spent at the IBM Scientific Center Heidelberg (Germany), in particular through his work in the ISO Prolog standardization committee, he recognized the potential of ASMs for building and verifying complex software-based systems in an effectively controllable manner, namely, by stepwise refinement of application-domain-focussed abstract ground models to executable code. Since then, he systematically pushed experiments to apply ASMs to real life, in particular industrial software-based systems. He triggered and led the effort of an international group of researchers which developed what is now known as the ASM method for high-level system design and analysis. He did this through multiple activities: through his own *research and publications* carried out at numerous research departments in Europe and the USA, through the *supervision of PhD students* in various European countries, through the definition and realization (including tool development) of academic and industrial *pilot projects* for building verifiable software in areas ranging from programming language implementation over train control to business processes [during sabbaticals at IBM 1989–1990,

[1] Details of the historical development can be found in the AsmBook [4, Ch.9].

Siemens Corporate Research and Development (Munich 1996, 1999), Microsoft Research (Redmond 2000), SAP Research (Karlsruhe, 2005)], through over 500 colloquium and conference *talks* worldwide and through the *organization* of:

- Seminars, e.g., the following Schloss Dagstuhl seminars:
  - *Methods for Semantics and Specification*, organized with Jean-Raymond Abrial (Paris), Hans Langmaack (University of Kiel, Germany), June 5–9, 1995. This seminar became known as the Steam-Boiler Seminar and resulted in a Springer LNCS State-of-the-Art Survey [6].
  - *Practical Methods for Code Documentation and Inspection*, organized with Paul Joannou (Ontario Hydro, Toronto, Canada), Dave Parnas (McMaster University, Canada), May 12–16, 1997.
  - *Requirements Capture/Documentation/Validation*, organized with Bärbel Hörger (Daimler-Benz Research, Germany), Dave Parnas (McMaster University, Canada), Dieter Rombach (Universität Kaiserslautern, Germany), June 14–18, 1999.
  - *Theory and Applications of Abstract State Machines*, organized with Andreas Blass (University of Michigan at Ann Arbor), Yuri Gurevich (Microsoft Research Redmond), March 4–8, 2002.
- Schools, e.g., the following summer schools:
  - *Informatica Matematica*, organized with Neil Jones (DIKU, University of Copenhague), Scuola Matematica Interuniversitaria, Cortona (Italy) July 9–30, 1989.
  - *Specification and Validation Methods for Programming Languages and Systems*, organized with Alfredo Ferro (University of Catania), Lipari (Sicily), June 21–July 3, 1993. See [7].
  - *Architecture Design and Validation Methods*, organized with Ferro (University of Catania), Lipari (Sicily) June 23–July 5, 1997. See [8].
  - *Formal Methods for Engineering of Software*, organized with Furio Honsell and Simone Martine (both University of Udine), CISM, Udine (Italy), September 24–28, 2001.
  - *Software Technology*, organized with Ferro (University of Catania), Lipari (Sicily) July 1–13, 2002.
  - *Advances in Software Engineering*, organized with Ferro (University of Catania), Lipari (Sicily), July 8–21, 2007. See [9].
- Workshops, including the series of (bi-)annual international ASM workshops. This series was started in 1993 at the IFIP World Computer Congress [10, Stream C] in Hamburg (Germany). Börger proposed at this Dagstuhl seminar, whose results are reported in this volume, to merge the regular meetings of the three major state-based formal method user groups, ASMs, B, and Z. This led to the establishment of the ABZ Conferences, the first of which took place in 2008 in London (UK) [11], to be followed by the next one in 2010 in Québec (Canada).

This list shows some of the altogether 25 books and special journal issues Börger edited and of over 30 international conferences, workshops, and schools

he organized in logic (1969–1989) and computer science (since 1990). His publications comprise over 100 research papers in logic (27) and computer science (89) and over 40 papers of technical expository or of epistemological character, written in English, German, French, and Italian. His major publications on ASMs are a book on the method [4] and a book on a characteristic application of the method to Java and its JVM implementation. The latter book exhibits all the main features of the ASM method, namely, (a) *building an abstract ground model* (read: a precise definition) that can be justified to faithfully formalize the language and machine requirements in SUN's manuals, (b) *horizontal and vertical refinements* leading from the ground model to executable code, (c) *validation* (by executing the models), and (d) *verification* (by mathematically proving or model checking properties of interest of the models, such as type safety, compiler correctness, and completness, etc.) [12].

In recognition of his pioneering work in logic and its applications in computer science, Börger was awarded the prestigious *Humboldt Research Award* in 2007–2008.

References

1. Börger, E.: Computability, Complexity, Logic (English translation of "Berechenbarkeit, Komplexität, Logik" from 1985. Vieweg-Verlag). Studies in Logic and the Foundations of Mathematics, vol. 128. North-Holland, Amsterdam (1989)
2. Börger, E., Grädel, E., Gurevich, Y.: The Classical Decision Problem. Perspectives in Mathematical Logic. Springer, Heidelberg (1997); Second printing in "Universitext". Springer, Heidelberg (2001)
3. Gurevich, Y.: Evolving algebras 1993: Lipari Guide. In: Börger, E. (ed.) Specification and Validation Methods, pp. 9–36. Oxford University Press, Oxford (1995)
4. Börger, E., Stärk, R.F.: Abstract State Machines. A Method for High-Level System Design and Analysis. Springer, Heidelberg (2003)
5. Gurevich, Y.: Sequential Abstract State Machines capture sequential algorithms. ACM Trans. Computational Logic 1, 77–111 (2000)
6. Abrial, J.R., Börger, E., Langmaack, H. (eds.): Formal Methods for Industrial Applications. Specifying and Programming the Steam Boiler Control. LNCS, vol. 1165. Springer, Heidelberg (1996)
7. Börger, E. (ed.): Specification and Validation Methods. Oxford University Press, Oxford (1995)
8. Börger, E. (ed.): Architecture Design and Validation Methods. Springer, Heidelberg (2000)
9. Börger, E., Cisternino, A. (eds.): Advances in Software Engineering. LNCS, vol. 5316. Springer, Heidelberg (2008)
10. Pehrson, B., Simon, I.: Technology/foundations. In: IFIP 13th World Computer Congress 1994. Elsevier, Amsterdam (1994)
11. Börger, E., Bowen, J., Butler, M., Boca, P. (eds.): ABZ 2008. LNCS, vol. 5238. Springer, Heidelberg (2008)
12. Stärk, R.F., Schmid, J., Börger, E.: Java and the Java Virtual Machine: Definition, Verification, Validation. Springer, Heidelberg (2001)

Rigorous Methods for Software Construction and Analysis

Dagstuhl Seminar 06191
May 7–12, 2006

We survey here the key objectives and the structure of the Dagstuhl Seminar 06191, which was organized as a Festkolloquium on the occasion of Egon Börger's 60th birthday, in May 2006 in Schloss Dagstuhl, Germany.

Focusing on applied formal methods, the final seminar program covered a wide range of applied research spanning from theoretical and methodological foundations to practical applications of Abstract State Machines, B, and beyond, emphasizing universal methods and tools that, regardless of their application orientation, are still committed to the ideal of mathematical rigor.

Two overarching themes were:

- The persistent demand to foster further cross-fertilization between academic research and industrial development in the quest for innovative methods and tools to critically evaluate their potential in the light of new challenges as posed by new technological developments and paradigms in software engineering.
- The ever-present question of convergence of methods, clarifying their commonalities and differences to better understand how to combine related approaches for accomplishing the various tasks in modeling, simulation, and verification of complex hardware/software systems.

In total, 54 participants from 14 different countries and four different continents attended the seminar. In 12 sessions, comprising a total of 35 presentations, 34 technical ones and one about fellowships and awards of the Alexander von Humboldt Foundation, the following central topics, among other topics, were addressed:

- Methodological foundations of requirements specification and verification
- Characterization of specification languages and their logical foundations
- Advanced tool environments and systematic integration of tools
- Machine-assisted validation and verification
- Distributed algorithms and concurrent protocols
- Novel applications in public safety, security, and privacy
- Industrial case studies and experience reports
- The role of formal methods in computer science education

The technical talks were either 30, 45, or 60 minutes and often resulted in lively and fruitful discussions which were continued informally during the breaks. After-dinner sessions were the norm, even on Wednesday after returning from an afternoon excursion to the charming historic town of Trier.

Overall the program was fairly balanced. Roughly,

- One third of the talks were related to Abstract State Machines
- One third of the talks were related to B
- One third to other formal methods and software engineering contexts

Rather than a strict grouping of talks according to research communities, technical content, and other standard criteria, the organizers deliberately chose a mixed program with the intention to stimulate interactions across research communities and also between industry and academia. This strategy turned out to be successful, as was evident from the impressive attendance of basically all the sessions with only very few exceptions.

Over the course of the seminar, a number of spontaneous requests for additional talks were brought forward. While not all of them could be accommodated due to given schedule restrictions, such dynamics provided further evidence of the inspiring and open atmosphere that also helped forge new collaborations. Notably, there was a concrete proposal for organizing a joint working conference on ASM, B, and Z in London in 2008.

Last but not least, the tremendous hospitality of Schloss Dagstuhl made the participants feel comfortable and helped create a pleasant atmosphere that allowed everyone to fully concentrate on research contributions for more than 12 hours a day. The organizers would like to express their sincere appreciation for all the support and specifically thank the terrific Dagstuhl staff for the their role in making this seminar so successful.

For the dissemination of results, revised and refereed versions of major contributions to the seminar were collected and published by Springer as an LNCS Festschrift.

October 2009

Jean-Raymond Abrial
Uwe Glässer

Referees

J.R. Abrial
R. Banach
J. P. Bowen
M. Butler
D. Cansell
A. Cavarra
A. Cisterino
N. Evans
R. Farahbod
V. Gervasi
U. Glässer
S. Hallerstede
T.S. Hoang
M. Leuschel
F. Mehta
D. Mery
P. Müller
W. Müller
M.-L. Potet
A. Prinz
S. Rastkar
E. Riccobene
D. Runje
J. N. Ruskiewicz
G. Schellhorn
K.-D. Schewe
S. Schneider
C. Snook
K. Stenzel
B. Thalheim
H. Treharne
M. Vajihollahi
L. Voisin
Ch. Wallace
J. Woodcock

Table of Contents