Lecture Notes in Computer Science 2757

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

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Bernhard K. Aichernig Tom Maibaum (Eds.)

Formal Methods at the Crossroads

From Panacea to Foundational Support

10th Anniversary Colloquium of UNU/IIST
the International Institute for Software Technology of
The United Nations University
Lisbon, Portugal, March 18-20, 2002
Revised Papers

Springer

Volume Editors

Bernhard K. Aichernig
UNU/IIST, The United Nations University
International Institute for Software Technology
P.O. Box 3058, Macao, China
E-mail: bka@iist.unu.edu

Tom Maibaum
King's College London, Department of Computer Science
Strand, London WC2R 2LS, United Kingdom
E-mail: tom@maibaum.org

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

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 Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): D.2, F.3, D.3, F.4

ISSN 0302-9743
ISBN 3-540-20527-6 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 10930748 06/3142 5 4 3 2 1 0

In Memoriam

Armando Martín Haeberer (1947–2003)

Preface

This volume records the 10th Anniversary Colloquium of UNU/IIST, the International Institute for Software Technology of the United Nations University, held in Lisbon, Portugal, March 18–21, 2002. Armando Haeberer, then Chairman of the board of UNU/IIST, conceived the idea of an international meeting in celebration of the institute's 10th anniversary. He was working in Lisbon at this time and he proposed to hold the meeting there, not least because the Portuguese government had been one of the major sponsors of the institute, right from the very beginning. The aim of the meeting, organized by the Board of UNU/IIST, was twofold. First, the institute's research work should be re-assessed and disseminated. Second, the future role of UNU/IIST's research area, formal methods, should be discussed.

Role of Formal Methods. Over at least three decades of development, the conception of what role formal methods should play in software engineering seems to have changed dramatically, influenced by both advocates and detractors. Beginning with a fundamentalist view that contested the genuineness of any 'non-formal' practice, dismissing it as an inappropriate contribution to the as yet ill-defined corpus of so-called software engineering, the conception of what this role should be has apparently evolved to a less naive engineering viewpoint. Today, as these theoretical methods acquire a new maturity and breadth of use, many of their advocates appear to be questioning their direct application by software practitioners, often considering it to be nonmandatory, and sometimes even nonadvisable. It appears that, together with the said maturation of the theoretical results and constructions, the perspective of their role within a far more complex picture of the software development activity has also matured. Today, many specialists and advocates of formal methods consider them as the framework that, by underlying the corpus of the software development praxis, lifts its status from craftsmanship to engineering, as happens in more classic branches of technology.

Aim and Shape of the Colloquium. UNU/IIST itself is located in Macao, near Hong Kong, at the heart of one of the major cultural and commercial crossroads of the world. In keeping with this multicultural focus, a group of approximately 30 eminent researchers from 15 countries on four continents gathered in Lisbon to cross swords and initiate the arduous task of tackling the colloquium's theme: *Formal Methods at the Crossroads: from Panacea to Foundational Support.* The meeting served as a forum for a thorough discussion of the inflexion point in the history of formal methods at which we currently find ourselves and an exploration of the potential changes to its very character. In addition to the group of active senior international scientists working in the area of formal methods and their application to software and hardware engineering, a group of young researchers and Ph.D. students were invited to participate. The reason for the existence of

the second group can be found in the very spirit of UNU/IIST, which is both a research and a training center of the UNU system.

The colloquium was organized as follows: First, the presentations were made and discussions took place among the best-known researchers, worldwide, in the area, interacting with young researchers and Ph.D. students. Second, the papers accompanying the presentations were discussed among the authors and the program committee while being written. Moreover, two scientists, who volunteered to do this, Profs. Carlo Ghezzi and Tom Maibaum, produced presentations to induce a couple of discussions that took place during the colloquium. In addition, the presentations and discussions were recorded and can be accessed at the postcolloquium site

http://www.iist.unu.edu/colloquium/

With satisfaction we see that the work initiated at this colloquium is currently being continued at a series of annual CUE workshops supported by agencies in China, Europe and the USA.

Contents of the Volume. The invited speakers at the colloquium and the participants from UNU/IIST were asked to submit a paper about the topic of their presentation. Most participants responded by indeed submitting said papers. Then, the tragic death of Armando Haeberer in February 2003 brought the process to a standstill for some time, as he had much of the material in his possession. It was subsequently agreed that we should proceed with the volume, but that some elements of Armando's vision could no longer be achieved, at least if we wanted to produce a timely volume. Hence, there are no introductory and concluding chapters by Armando, Tom Maibaum and Carlo Ghezzi, which were intended to be a commentary on and analysis of the contents of the papers and what was said at the colloquium. As the meeting was recorded, it had also been Armando's hope to integrate the transcription of the audio tapes into the volume itself, to provide further context and analysis for the papers. Again, unfortunately, we could not proceed with this. The submitted papers were reviewed by the participating invited speakers.

Hence, the volume is more conventional than had been intended. It is organized into 6 parts. The first paper in the volume is a recollection of Armando Haeberer's life by Tom Maibaum. The second part, entitled 'Work at UNU/IIST,' contains a paper by Zhou Chaochen, then Director of the Institute (and now retired) about the Institute, its history and its present work. Then there are several papers illustrating the research ongoing at the Institute. There is a paper by its newest Research Fellow, Bernhard Aichernig, about a formal-methods-based approach to testing. The idea of contracts, as seen in the work of Bertrand Meyer, amongst others, is extended to tests, seen as an operational contract. It is shown how tests can be derived via refinement techniques from specification contracts.

Chris George, now Director ad interim of the Institute, describes work on the RAISE tools and method. The focus is on deriving a design specification from the requirements. He Jifeng describes how the hardware specification language

VERILOG can be characterized algebraically and how this algebraic characterization leads to operational and denotational presentations of the language. Dang Van Hung then reviews the development of the Duration Calculus, which can be used to describe and analyze real-time systems. Tomasz Janowski then describes the language X2Rel and its semantics. The purpose of the language is to enable the description of many different kinds of binary relations between XML documents.

In the next section, entitled 'At the Crossroads,' we see a number of papers that tried to directly address the theme of the colloquium, i.e., the state of the art in software engineering and its basis in proper engineering/scientific principles. The title of the paper by Michael Jackson, 'Where, Exactly, Is Software Development?,' directly focuses on the problem of characterizing and analyzing the context of the software to be built. How can one formalize the context and its relationship to the software? Michael sees this as an important challenge for the subject. The paper by Astesiano, Reggio and Cerioli uses reflections by the authors of their experience and knowledge of practical software engineering to propose software development methods that more purposefully integrate the use of formal techniques. Tony Hoare proposes a challenge for software development: making a verifying compiler. The idea is that a compiler proves the correctness of a program before 'allowing it to run.' This is aided by assertions attached to the program and, of course, appropriate and automatic verification technology.

J Strother Moore puts forward another grand challenge for formal methods: to build and mechanically verify a practical software system, from the transistor level right to the application software. He sees this as being beyond the capacity of any single person or group and requiring both competition and collaboration. However, he sees the benefits to the subject as being of major proportions. Dines Bjørner addresses the problems and role of domain engineering and, in particular, the importance and role of infrastructure components and an associated notion of transaction script workflows. (He also devotes some space to reflections on the 10 years of UNU/IIST's existence.) The paper by Cliff Jones on the formalization of some dependability notions concludes the section. He identifies the concept of system as an important focus, together with the genesis of a system from other systems. He characterizes concepts such as fault, error and failure in the framework.

The section 'From Models to Software' begins with a paper by Manfred Broy on the role of models and views in program development. His paper includes a comprehensive family of software models as well as a discussion on how these models are related. The section continues with a paper by Thiagarajan and Roychoudhury on message sequence charts. Their concern is the establishment of a relationship between the language of message sequence charts and an executable language. They propose Cyclic Transition Processes to fill this gap. Ferrari, Montanari and Tuosto use hypergraphs and graph synchronization to model wide area network applications. Their longer-term objective is to provide software engineering tools for designing and certifying internetworking systems. The paper by Pavlovic and Smith rehearses the ongoing work at the Kestrel

Institute on support for the formal development of software, focusing on refinement concepts. The underlying mathematical framework is based on a category of higher-order specifications, and refinement is implemented via the construction of colimits.

Bailes and Kemp describe their 'totally functional approach to programming,' consisting of the representation of data structures in terms of 'platonic combinators,' which have some nice formal properties. The paper by José Fiadeiro concludes the section by describing the use of co-ordination technologies in support of the evolution of systems. The claim is that most systems are not built as new, but rather are evolved from some previous system. The key is the externalization of interaction between components so as to more easily assemble and extend systems built in this way.

The next section contains papers focusing on real-time systems. The paper by Yingxu Wang describes real-time process algebra. The language addresses operations, event/process timing and memory manipulation, and the paper also provides examples of its use. Chen and Lin describe a formalism based on communicating timed automata. The language enables the expression of real-time constraints and data communication, and the language has a graphical representation. The paper by David, Behrmann, Larsen and Wang Yi describes the architecture of a new implementation of the model-checking tool Uppaal. The design is based on a pipeline architecture and a single shared data structure. The design decisions are supported by experimental evidence.

The final section is on verification. The paper by Shankar looks at the problem of combining the effectiveness of model checking, with its limitations due to the size of state spaces, and deductive theorem proving methods, with their limitations on automation. The method proposed is based on abstracting from a specification a finite state approximation of the program that preserves the property of interest by using deductive methods. Then, model checking can be used to provide assurance of the proper working of the program with respect to that property. The paper by Manna and Zarba gives a survey of what is known about combining decision procedures, in particular in relation to combining theories over nondisjoint signatures. Kaltenbach and Misra address the problem of model checking progress properties of systems. These kinds of properties are usually difficult to check as they involve doubly nested fixed points. They propose the addition of 'hints,' expressed as regular expressions over the language of actions of a program. Finally, in his paper Naoki Kobayashi extends type systems to concurrent programs to analyze deadlock freedom, safe usage of locks, etc.

We hope that the readers of this volume benefit scientifically from these proceedings and also find it stimulating for clarifying the role of formal methods in their research.

July 2003

Bernhard K. Aichernig
Tom Maibaum

Keynote Speakers

The list of invited participants includes some of the most well-known researchers in the area of formal methods and their applications. They are:

- Prof. Egidio Astesiano (University of Genoa, Italy)
- Prof. Paul Bailes (University of Queensland, Australia)
- Prof. Dines Bjørner (Technical University of Denmark, Denmark)
- Dr. Dominique Bolignano (Trusted Logic, France)
- Prof. Manfred Broy (Technische Universität München, Germany)
- Prof. Fu Yuxi (Department of CS, Shanghai JiaoTong University, People's Republic of China)
- Prof. José Luiz Fiadeiro (ATX Software and University of Lisbon, Portugal)
- Prof. Carlo Ghezzi (Politecnico di Milano, Italy)
- Dr. Constance Heitmeyer (US Naval Research Laboratory, USA)
- Prof. Tom Henzinger (University of Berkeley, USA)
- Prof. C.A.R. Hoare (Microsoft Research, Cambridge, UK)
- Prof. Michael Jackson (Open University, UK)
- Prof. Cliff Jones (University of Newcastle upon Tyne, UK)
- Prof. Gilles Kahn (INRIA, France)
- Dr. Naoki Kobayashi (Tokyo Institute of Technology, Japan)
- Prof. Lin Huimin (Chinese Academy of Sciences, Beijing, People's Republic of China)
- Prof. Tom Maibaum (King's College London, UK)
- Prof. Ugo Montanari (Università di Pisa, Italy)
- Prof. David Parnas (McMaster University, Canada)
- Prof. Amir Pnueli (Weizmann Institute of Science, Israel)
- Dr. Natarajan Shankar (SRI International, USA)
- Dr. Douglas Smith (Kestrel Institute, USA)
- Prof. P.S. Thiagarajan (Chennai Mathematical Institute, India)
- Prof. Wang Yi (Chinese Academy of Sciences, People's Republic of China and Uppsala University, Sweden)
- Prof. Yingxu Wang (University of Calgary, Canada)

The following academic staff of UNU/IIST participated:

- Prof. Zhou Chaochen, Director
- Chris George, Senior Research Fellow
- Prof. He Jifeng, Senior Research Fellow
- Dr. Bernhard K. Aichernig, Research Fellow
- Dr. Dang Van Hung, Research Fellow
- Dr. Tomasz Janowski, Research Fellow

Program Committee

The organization of the colloquium was the responsibility of a program committee, isomorphic to the membership of the UNU/IIST Board at the time.

Chairman	Armando Haeberer (ATX Software, Portugal and King's College London, UK)
Vice-Chairman	Mathai Joseph (Tata Institute, India)
Members	Ibrahim Eissa (University of Cairo, Egypt)
	Hans van Ginkel (Rector of UNU, Japan)
	Gerard Huet (INRIA, France)
	Iu Vai Pan (University of Macau, China)
	Zohar Manna (Stanford University, USA)
	Pedro Manuel Barbosa Veiga (University of Lisbon, Portugal)
	Wu Ying Jian (Ministry of Science and Technology, China)
	Zhou Chaochen (Director of UNU/IIST, China)

Executive Committee

The program committee delegated the executive organization to the executive committee.

Members	José Luiz Fiadeiro (ATX Software and University of Lisbon, Portugal)
	Armando Haeberer

In addition, the following people helped particularly with the organization of the colloquium in various capacities:

Technical Organization	Miguel Costa (ATX Software)
Administrative Organization	Cristina Teles (ATX Software)
Organization at UNU/IIST	Hoi Iok Wa, Wendy
	Pun Chong Iu, Alice
	Ho Sut Meng, Michelle
	Chan Iok Sam, Kitty

Support

We are grateful for the support of the following organizations:

- ATX Software (Portugal)
- European Commission
- Fundação para a Ciência e a Tecnologia (Portugal)
- Gabinete de Relações Internacionais da Ciência e do Ensino Superior (Portugal)
- University of Lisbon

Table of Contents

From Models to Software

Real-Time Systems

Verification