



**Springer**

*Berlin*

*Heidelberg*

*New York*

*Barcelona*

*Hong Kong*

*London*

*Milan*

*Paris*

*Singapore*

*Tokyo*

Teodor Rus (Ed.)

# Algebraic Methodology and Software Technology

8th International Conference, AMAST 2000  
Iowa City, Iowa, USA, May 20-27, 2000  
Proceedings



Springer

## Series Editors

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

## Volume Editor

Teodor Rus  
The University of Iowa, Department of Computer Science  
Iowa City, IA 52242, USA  
E-mail: rus@cs.uiowa.edu

## Cataloging-in-Publication Data applied for

## Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Algebraic methodology and software technology : 8th international conference ; proceedings / AMAST 2000, Iowa City, Iowa, USA, May 20 - 27, 2000. Teodor Rus (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2000  
(Lecture notes in computer science ; Vol. 1816)  
ISBN 3-540-67530-2

CR Subject Classification (1998): F.3-4, D.2, C.3, D.1.6, I.2.3, I.1.3

ISSN 0302-9743

ISBN 3-540-67530-2 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 is a company in the BertelsmannSpringer publishing group.  
© Springer-Verlag Berlin Heidelberg 2000  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Boller Mediendesign  
Printed on acid-free paper      SPIN: 10720319      06/3142      5 4 3 2 1 0

# Preface

The AMAST movement was initiated in 1989 with the First International Conference on Algebraic Methodology and Software Technology (AMAST), held on May 21–23 in Iowa City, Iowa, and aimed at setting the development of software technology on a mathematical basis. The virtue of the software technology envisioned by AMAST is the capability to produce software that has the following properties: (a) it is correct and its correctness can be proved mathematically, (b) it is safe, such that it can be used in the implementation of critical systems, (c) it is portable, i.e., it is independent of computing platforms and language generations, and (d) it is evolutionary, i.e., it is self-adaptable and evolves with the problem domain. Ten years later a myriad of workshops, conferences, and research programs that share the goals of the AMAST movement have occurred. This can be taken as proof that the AMAST vision is right. However, often the myriad of workshops, conferences, and research programs lack the clear objectives and the coordination of their goals towards the software technology envisioned by AMAST. This can be taken as a proof that AMAST is still necessary.

The approach of software development promoted by AMAST is based on the integration of the two fundamental mechanisms for problem solving, *specification* and *computation*, into a general problem-solving model by a machine-independent methodology where: (1) specification allows one to develop the mathematical model of the problem at hand and to represent this model in a mathematical language; (2) computation allows one to apply specific *calculi* on problem representation and its input data to deduce the solution. A major aspect of the AMAST interpretation of the algebraic methodology is that software environments designed to help develop software systems should be populated by tools, components, and patterns. Tools are efficient implementations of universal algorithms; components are stand-alone software automatically generated by tools from finite specifications; patterns are domain-oriented composition schemes mapping components into software systems. This ensures the development of a software factory capable of producing software systems having the qualities required by the AMAST movement.

Ten years after its initiation AMAST is no longer a simple grass-roots movement. Instead, AMAST has become a professional movement whose goals are embraced by a large international following. As long as AMAST remains a movement of world-wide computer science researchers determined by philosophical and intellectual conviction rather than by academic or business opportunism, AMAST can provide the balance and the common sense needed by the myriad of formal-methods trends, that are often short sighted by short-term goals of for-profit-organizations. This makes AMAST further necessary as the unique worldwide movement with the goal of *creating the mathematical methodology for the development of software technology*. The transformation of algebraic methodology into the software technology is a dynamic process that involves both static

and evolutionary knowledge. Since the more one discovers the more remains to be discovered this process never ends. Hence, AMAST will always be needed to balance the process of building the software factory.

In response to the call for papers, 53 papers were submitted to AMAST 2000 and 29 have been selected by the program committee. The relatively small number of papers submitted tells us that the recent advances in software system design and application requires new forms of research dissemination. It seems that the classical form of paper presentation cannot catch the excitement raised by the current stage of the software technology. Therefore AMAST 2000 takes a step ahead on research dissemination by mixing paper presentations with open panel discussions. The discussion of the software worker education is guided by David Lorge Parnas, who introduces us to “A software engineering program of lasting value” and Jeannette M. Wing, who presents “Thoughts on integrating formal methods into a computer science curriculum”. The technical meetings are organized around the following invited talks: Egidio Astesiano, “Plugging data constructs into paradigm-specific languages: towards an application to UML”; Yuri Gurevich, “ASM formalware in the software engineering cycle”; Michael Healy, “Applying category theory to derive engineering software from encoded knowledge”; Oege de Moor, “Pointwise relational programming”; David Lorge Parnas, “Making mathematical methods more practical for the software developer”; and Martin Wirsings, “Algebraic state machines”. The excitement is however provided by the three open-panel discussions organized by Joseph Goguen, “New computing logics”; Douglas Smith, “Automatic program generation”; and Roger Shultz, “From software model to commercial product”. We thank all these invited speakers for sharing their expertise with us.

Here I thank those whose generosity made possible the organization of this AMAST conference. Ralph Wachter, Office of Naval Research, helped us to initiate AMAST, to lead it towards its maturity, and finally to celebrate its 10th anniversary. Thanks are due to the University of Iowa, Dean Linda Maxson, Associate Provost Lee Anna Clark, and Vice President for Research David Skorton, for their financial support, and particularly Steve Bruell, Chair of Computer Science Department, for his continual support. I also thank Arthur Fleck and the AMAST steering committee for the guidance and all the program committee members for their effort during paper reviewing and selection. Finally, I thank all those who submitted papers to this edition of AMAST. I believe that the result of a peer-evaluation process is rather subjective and therefore I congratulate both those whose papers were accepted as well those whose papers were not accepted. Last (of course, not least) my thanks go to the organizing committee, particularly to Robert Kooima, and to Springer-Verlag, particularly to Alfred Hofmann, Anna Kramer, and Antje Endemann, whose excellent cooperation and advice made these proceedings feasible.

# Organization

**Conference chair:** Maurice Nivat

**Program chair:** Teodor Rus

**Local organization chair:** Steve Bruell

## Program Committee

Andre Arnold, France	Egidio Astesiano, Italy
Gabriel Baum, Argentina	Didier Begay, France
Robert Berwick, USA	Michel Bidoit, France
Val Tannen, USA	Gregor Bochmann, Canada
Chris Brink, South Africa	Manfred Broy, Germany
Christian Calude, New Zealand	Christine Choppy, France
Philippe Darondeau, France	Jim Davies, UK
Rocco De Nicola, Italy	Ruy de Queiroz, Brazil
Arthur Fleck, USA	Marcelo Frias, Argentina
Kokichi Futatsugi, Japan	Dov Gabbay, UK
Harald Ganzinger, Germany	Radu Grosu, USA
Yuri Gurevich, USA	Armando Haeberer, Brazil
Nicolas Halbwachs, France	Michael Healy, USA
Peter Henderson, UK	Yoshi Inagaki, Japan
Paola Inverardi, Italy	Dan Ionescu, Canada
Ryszard Janicki, Canada	Jarkko Kari, USA
Michael Johnson, Australia	Helene Kirchner, France
Gary Leavens, USA	Luigi Logrippo, Canada
Thomas Maibaum, UK	Zohar Manna, USA
Chris Marlin, Australia	Michael Mislove, USA
Peter Mosses, Denmark	George Nelson, USA
Anton Nijholt, The Netherlands	Maurice Nivat, France
Michael O'Donnell, USA	Fernando Orejas, Spain
David Lorge Parnas, Canada	Sriram Pemmaraju, India
Don Pigozzi, USA	Jacques Printz, France
Charles Rattray, UK	Teodor Rus, USA
Giuseppe Scollo, The Netherlands	Stephen Seidman, USA
Roger Shultz, USA	Ken Slonneger, USA
Douglas Smith, USA	John Staples, Australia
Carolyn Talcott, USA	Andrzej Tarlecki, Poland
Alagar Vangalur, Canada	Rob van Glabbeek, USA
Paulo Veloso, Brazil	Brian Warboys, UK
Jeannette Wing, USA	Martin Wirsing, Germany
Hantao Zhang, USA	

## Steering Committee

E. Astesiano	R. Berwick	Z. Manna
M. Mislove	A. Nijholt	M. Nivat
J. Printzs	C. Rattray	T. Rus
G. Scollo	J. Staples	J. Wing
M. Wirsing		

## Organizing Committee

A. Fleck	R. Kooima	T. Rus
----------	-----------	--------

## Referees

V.S. Alagar	A. Arnold	G. Baum
M. Bidoit	M. Boreale	M. Breitling
C. Calude	A. Cerone	P. R. D'Argenio
P. Darondeau	J. Davies	D. Eichmann
C. Fidge	A. Fleck	M. Frias
H. Ganzinger	R. Grosu	N. Halbwachs
M. Healy	P. Henderson	P. Inverardi
D. Ionescu	R. Janicki	M. Johnson
J. Kari	C. Kirchner	M. Koutny
I. Kreuger	G. Leavens	L. Logrippo
M. Loreti	S. Maharaj	F. Maraninchi
C. Marlin	P.E. Martinez Lopez	M. Mislove
L. Moss	P. Mosses	G. Nelson
A. Nijholt	M. O'Donnell	F. Orejas
D. Pigozzi	R. Pugliese	C. Rattray
G. Rosolini	T. Rus	P. Schnoebelen
G. Scollo	S. Seidman	H. Sipma
K. Slonneger	G. Smith	C. Talcott
A. Tarlecki	R. van Glabbeek	B. Warboys
M. Wirsing	H. Zhang	

## Sponsoring Institutions

The University of Iowa  
Office of Naval Research

# Contents

---

## Education Day

---

<b>Invited Talk:</b> A Software Engineering Program of Lasting Value . . . . .	1
<i>David L. Parnas</i>	
<b>Invited Talk:</b> Weaving Formal Methods into the Undergraduate Computer Science Curriculum . . . . .	2
<i>Jeannette M. Wing</i>	

---

## Technical Meetings

---

### Session 1

<b>Invited Talk:</b> Making Mathematical Methods More Practical for the Software Developers . . . . .	9
<i>David L. Parnas</i>	
Step by Step to Histories . . . . .	11
<i>Max Breitling, Jan Philipps</i>	
Distance Functions for Defaults in Reactive Systems . . . . .	26
<i>Sofia Guerra</i>	
Generalizing the Modal and Temporal Logic of Linear Time . . . . .	41
<i>Bernhard Heinemann</i>	
Process Algebra versus Axiomatic Specification of a Real-Time Protocol . .	57
<i>Antonio Cerone</i>	
Practical Application of Functional and Relational Methods for the Specification and Verification of Safety Critical Software . . . . .	73
<i>Mark Lawford, Jeff McDougall, Peter Froebel, Greg Moun</i>	

### Session 2

<b>Invited Talk:</b> Algebraic State Machines . . . . .	89
<i>Manfred Broy, Martin Wirsing</i>	
Meta Languages in Algebraic Compilers . . . . .	119
<i>Eric Van Wyk</i>	
Random Access to Abstract Data Types . . . . .	135
<i>Martin Erwig</i>	

A Monad for Basic Java Semantics .....	150
<i>Bart Jacobs, Erik Poll</i>	
A Global Semantics for Views .....	165
<i>Christine Choppy, Pascal Poizat, Jean-Claude Royer</i>	
Analysis of Downward Closed Properties of Logic Programs .....	181
<i>Patricia M. Hill, Fausto Spoto</i>	

### Session 3

<b>Invited Talk:</b> ASM Formalware in the Software Engineering Cycle .....	197
<i>Yuri Gurevich</i>	
Process Calculi for Coordination: From Linda to JavaSpaces .....	198
<i>Nadia Busi, Roberto Gorrieri, Gianluigi Zavattaro</i>	
The Algebra of Multi-tasking .....	213
<i>Colin J. Fidge</i>	
A Causal Semantics for Timed Default Concurrent Constraint Programming .....	228
<i>Simone Tini, Andrea Maggiolo-Schettini</i>	
CASL-CHART: A Combination of Statecharts and of the Algebraic Specification Language CASL .....	243
<i>Gianna Reggio, Lorenzo Repetto</i>	
Message Authentication through <i>Non Interference</i> .....	258
<i>Riccardo Focardi, Roberto Gorrieri, Fabio Martinelli</i>	

### Session 4

<b>Invited Talk:</b> Plugging Data Constructs into Paradigm-Specific Languages: Towards an Application to UML .....	273
<i>Egidio Astesiano, Maura Cerioli, Gianna Reggio</i>	
An ASM Semantics for UML Activity Diagrams .....	293
<i>Egon Börger, Alessandra Cavarra, Elvinia Riccobene</i>	
Approximate Bisimilarity .....	309
<i>Mingsheng Ying, Martin Wirsing</i>	
Time and Probability in Process Algebra .....	323
<i>Suzana Andova</i>	
A Modal Logic for KLAIM .....	339
<i>Rocco De Nicola, Michele Loreti</i>	

Kleene under a Demonic Star .....	355
<i>Jules Desharnais, Bernhard Möller, Fairouz Tchier</i>	

## Session 5

<b>Invited Talk:</b> Pointwise Relational Programming .....	371
<i>Oege de Moor, Jeremy Gibbons</i>	
Towards a Toolkit for Actor System Specification .....	391
<i>Carolyn L. Talcott</i>	
Maude Action Tool: Using Reflection to Map Action Semantics to Rewriting Logic .....	407
<i>Christiano de O. Braga, E. Hermann Haeusler, José Meseguer, Peter D. Mosses</i>	
The Extensibility of Maude's Module Algebra .....	422
<i>Francisco Durán</i>	
A Reuse-Oriented Framework for Hierarchical Specifications .....	438
<i>Sophie Coudert, Pascale Le Gall</i>	
MIX(FL): A Kernel Language of Mixin Modules .....	454
<i>Davide Ancona</i>	
Behavioural Subtyping Relations for Object-Oriented Formalisms .....	469
<i>Clemens Fischer, Heike Wehrheim</i>	

## Session 6

<b>Invited Talk:</b> Applying Category Theory to Derive Engineering Software from Encoded Knowledge .....	484
<i>Michael Healy, Keith Williamson</i>	
A New Logic for Electronic Commerce Protocols .....	499
<i>Kamel Adi, Mourad Debbabi, Mohamed Mejri</i>	
Extended Institutions for Testing .....	514
<i>Marielle Doche, Virginie Wiels</i>	
Testing from Structured Algebraic Specifications .....	529
<i>Patrícia D. L. Machado</i>	
<b>Author Index</b> .....	545