Lecture Notes in Computer Science 1101
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Advisory Board: W. Brauer D. Gries J. Stoer

Martin Wirsing Maurice Nivat (Eds.)

Algebraic Methodology and Software Technology

5th International Conference, AMAST '96
Munich, Germany, July 1-5, 1996
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Martin Wirsing
Ludwig-Maximilians-Universität München, Institut für Informatik
Oettingenstr. 67, D-80538 München, Germany

Maurice Nivat
LITP, Université Paris XII - Denis Diderot
2, Place Jussieu, F-75005 Paris, France

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Algebraic methodology and software technology : 5th international conference ; proceedings / AMAST '96, Munich, Germany, July 1 - 5, 1996. Martin Wirsing ; Maurice Nivat (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1996
(Lecture notes in computer science ; Vol. 1101)
ISBN 3-540-61463-X
NE: Wirsing, Martin [Hrsg.]; AMAST <5, 1996, München>; GT

CR Subject Classification (1991): F.3-4, D.2, C.3, D.1.6, I.2.3, H.2.1-4

ISSN 0302-9743
ISBN 3-540-61463-X 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 1996
Printed in Germany

Typesetting: Camera-ready by author
SPIN 10513306 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

This volume contains the contributions of invited speakers, refereed papers, and reports on system presentations of the Fifth International Conference on Algebraic Methodology and Software Technology (AMAST '96) held in Munich, July 1-5, 1996. The previous four editions of AMAST took place at the University of Iowa (USA) in 1989 and 1991, at the University of Twente (The Netherlands) in 1993, and at the University of Montreal (Canada) in 1995.

The major goals of the AMAST conferences are to put software development technology on a firm, mathematical foundation. Particular emphasis is given to algebraic and logical foundations of software technology. An eventual goal is to establish algebraic and logical methodology as a practically viable and attractive alternative to the prevailing ad hoc approaches to software engineering.

As in the previous years the first day of AMAST '96 was dedicated to the education of software engineers. The theme this year was on applications of formal methods in industrial software development showing the use of mathematics-based methods to give support for requirement analysis, formal specification, and design.

In response to the call for papers, 67 papers were submitted. We invited six speakers for the education day, six speakers for the conference days, and one speaker for the banquet. The Program Committee met on January 29 and accepted 25 papers, complemented by an almost equal number of 23 system demonstrations.

The distinguished invited speakers are André Arnold, Jan Bergstra, Gérard Berry, Manfred Broy, Arie van Deursen, José Fiadeiro, John Fitzgerald, Eric Hehner, Bernd Krämer, Dino Mandrioli, Sriram Sankar, and Douglas Smith. We are also fortunate to have F.L. Bauer as our banquet speaker.

The accepted papers cover the major conference themes: algebraic and logical foundations, concurrency, software technology, and logic programming. The subjects of these papers include a wide variety of methods, notations, semantics, and proofs contributing to an advancement and rigorous development of software systems. The reports on system presentations describe ongoing research efforts to implement algebraic and logical methods and to apply formal methods in software technology.

On behalf of the Program Committee I would like to thank all those who submitted papers and system presentations and the referees who helped to evaluate the papers.

The support of DFG (Deutsche Forschungsgemeinschaft),
Münchener Universitätsgesellschaft,
sd&m,
Versicherungskammer Bayern/Bayen-Versicherung,
Siemens AG
is gratefully acknowledged. Rolf Hennicker, Christian Baur, Alexander Kurz, Luis Mandel, Bernhard Reus, Weishi Zhang, Marianne Diem, Agnes Szabo-Lackinger, Thomas Lackinger, and several other members of the department provided invaluable help throughout the preparation and organization of the conference. I also would like to thank Alfred Hofmann at Springer-Verlag for his excellent cooperation concerning the publication of this volume.

Munich, April 1996

Martin Wirsing

Program Chair: Martin Wirsing

Program Committee
Martin Abadi (USA)
V.S. Alagar (Canada)
Egidio Astesiano (Italy)
Didier Begay (France)
Gregor Bochmann (Canada)
Chris Brink (South Africa)
Bruno Buchberger (Austria)
Kokichi Futatsugi (Japan)
Harald Ganzinger (Germany)
Armando Haeberer (Brazil)
Nicolas Halbwachs (France)
Yasuyoshi Inagaki (Japan)
Paola Inverardi (Italy)
Mike Johnson (Australia)
Helene Kirchner (France)
Tom Maibaum (UK)
Jan Maluszynski (Sweden)
Josè Meseguer (USA)
Peter Mosses (Denmark)
Rocco De Nicola (Italy)
Anton Nijholt (The Netherlands)
Fernando Orejas (Spain)
R. Ramanujam (India)
Charles Rattray (UK)
Teodor Rus (USA)
Giuseppe Scollo (The Netherlands)
R.K. Shyamasundar (India)
Andrzej Tarlecki (Poland)
Herbert Weber (Germany)

General Chair: Maurice Nivat

Organizing Committee
Chair: Martin Wirsing (Germany)

Tools and Demos:
Christian Baur (Germany)

Publicity:
Charles Rattray (UK)
V.S. Alagar (Canada)
Michel Bidoit (France)
Jacques Printz (France)
Teodor Rus (USA)
Giuseppe Scollo (The Netherlands)

Local Arrangements:
Rolf Hennicker (Germany)
Marianne Diem (Germany)

Subreferees

The program committee members and a number of external referees refereed all submitted papers and helped in the selection of papers from among the many excellent submissions received. Their invaluable timely reports and assistance during the selection process made it possible to bring the proceedings to its present form.

A. Arnold
D. Basin
H. Baumeister
B. Berthomieu
P. Bhaduri
A. Bockmayr
A. Borusan
A.M. Borzyszkowski
A. Bouajjani
G. Boudol
J. Boye
P. van den Broek
R. Buckland
L. Campora
M. Carlsson
P. Caspi
I. Castellani
P. Casteran
C. Castro
I. Claßen
D. Craigen
P. Degano
S.M. Eker
G. Ferrari
M. Fokkinga
P. Freedman
B. Gramlich
A. Griffault
H. Hong
S.B. Jones
J-P. Katoen
F. Khendek
A. Khoumsi
M. Klar
B. Konikowska
R. Kubiak
K.N. Kumar
J. Kuper
R-D. Kutsche
A. Labella
Y. Lakhnech
R. Langerak
B. Le Saec
P. Lincoln
K. Lodaya
G. Malcolm
O. Maler
C. Marché
R. Mateescu
C. Meo
S.K. Mohalik
M. Mukund
T. Naoi
M. Nesi
F. Nickl
W. Pawlowski
M. Peixoto
A. Petrenko
A. Pierantonio
M. Poel
F.P. Presicce
C. Priami
R. Pugliese
M.R.K. Krishna Rao
G. Reggio
G. Richard
F. Rossi
M. Rusinowitch
T. Sakabe
L. Scott
M. Sighireanu
R. de Simone
S. Sokolowski
S. Tai
P.S. Thiagarajan
E. Tronci
P.A. Wacrenier
S. Wasserroth
D. Wolz
S. Yuen
M.V. Zilli
E. Zucca
J. Zwiers

Table of Contents

Education Day: Industrial Applications of Formal Methods

Two Industrial Trials of Formal Specification 1
J.S. Fitzgerald

Industrial Applications of ASF+SDF 9
M. van den Brand, A. van Deursen, P. Klint, S. Klusener, E. van der Meulen

The Embedded Software of an Electricity Meter: An Experience in Using Formal Methods in an Industrial Project 19
A. Arnold, D. Bégay, J.-P. Radoux

Applying Research Results in the Industrial Environment: The Case of the TRIO Specification Language 33
D. Mandrioli

Using Heterogeneous Formal Methods in Distributed Software Engineering Education 43
B.J. Krämer

Introducing Formal Methods to Software Engineers Through OMG's CORBA Environment and Interface Definition Language 52
S. Sankar

Conference

Invited Talk: *Toward a Classification Approach to Design* 62
D.R. Smith

Session 1: Theorem Proving

Semantic Foundations for Embedding HOL in Nuprl 85
D.J. Howe

Free Variable Tableaux for a Many Sorted Logic with Preorders 102
A. Gavilanes, J. Leach, S. Nieva

Automating Induction over Mutually Recursive Functions 117
D. Kapur and M. Subramaniam

Session 2: Algebraic Specification

Pushouts of Order-Sorted Algebraic Specifications 132
A.E. Haxthausen and F. Nickl

A Formal Framework for Modules with State 148
D. Ancona and E. Zucca

Object-Oriented Implementation of Abstract Data Type Specifications 163
R. Hennicker and C. Schmitz

Session 3: Concurrent and Reactive Systems I

On the Completeness of the Equations for the Kleene Star in Bisimulation 180
W. Fokkink

An Equational Axiomatization of Observation Congruence for Prefix Iteration 195
L. Aceto and A. Ingólfsdóttir

Finite Axiom Systems for Testing Preorder and De Simone Process Languages 210
I. Ulidowski

Invited Talk: *Constructive Semantics of Esterel: From Theory to Practice* 225
G. Berry

Session 4: Program Verification

Using Ghost Variables to Prove Refinement 226
M. Marcus and A. Pnueli

Tracing the Origins of Verification Conditions 241
R. Fraer

Preprocessing for Invariant Validation 256
E.P. Gribomont

Formal Verification of SIGNAL Programs: Application to a Power Transformer Station Controller 271
M. Le Borgne, H. Marchand, É. Rutten, M. Samaan

Invited Talk: *The Discrete Time TOOLBUS* 286
J.A. Bergstra and P. Klint

Session 5: Concurrent and Reactive Systems II

A Study on the Specification and Verification of Performance Properties 306
X.J. Chen, F. Corradini, R. Gorrieri

Symbolic Bisimulation for Timed Processes 321
M. Boreale

Approximative Analysis by Process Algebra with Graded Spatial Actions 336
Y. Isobe, Y. Sato, K. Ohmaki

Invited Talk: *Boolean Formalism and Explanations* 351
E.C.R. Hehner

Session 6: Logic Programming and Term Rewriting

Proving Existential Termination of Normal Logic Programs 375
M. Marchiori

Programming in Lygon: An Overview 391
J. Harland, D. Pym, M. Winikoff

Some Characteristics of Strong Innermost Normalization 406
M.R.K. Krishna Rao

Invited Talk: *On the Emergence of Properties in Component-Based Systems* 421
J.L. Fiadeiro

Session 7: Algebraic and Logical Foundations

Algebraic View Specification 444
B. Paech

Towards Heterogeneous Formal Specifications 458
G. Bernot, S. Coudert, P. Le Gall

A Categorical Characterization of Consistency Results 473
C. Baier and M. Majster-Cederbaum

Invited Talk: *Algebraic Specification of Reactive Systems* 487
M. Broy

Session 8: Concurrent and Reactive Systems III

A Model for Mobile Point-to-Point Data-flow Networks without Channel Sharing 504
R. Grosu and K. Stølen

Coalgebraic Specifications and Models of Deterministic Hybrid Systems 520
B. Jacobs

A Bounded Retransmission Protocol for Large Data Packets 536
J.F. Groote and J. van de Pol

System Presentations

SPECWARE: An Advanced Environment for the Formal Development of Complex Software Systems 551
R. Juellig, Y. Srinivas, J. Liu

ASSPEGIQUE$^+$: An Integrated Specification Environment Providing Inter-Operability of Tools 555
M. Bidoit, C. Choppy, F. Voisin

Towards Integrating Algebraic Specification and Functional Programming: the Opal System 559
K. Didrich, C. Gerke, W. Grieskamp, C. Maeder, P. Pepper

InterACT: An Interactive Theorem Prover for Algebraic Specifications 563
R. Geisler, M. Klar, F. Cornelius

A New Proof-Manager and Graphic Interface for the Larch Prover 567
F. Voisin

TERSE: A Visual Environment for Supporting Analysis, Verification and Transformation of Term Rewriting Systems 571
N. Kawaguchi, T. Sakabe, Y. Inagaki

The TOOLBUS Coordination Architecture: A Demonstration 575
P. Klint and P. Olivier

ASD: The Action Semantic Description Tools 579
A. van Deursen and P.D. Mosses

Using Occurrence and Evolving Algebras for the Specification of Language-Based Programming Tools 583
A. Poetzsch-Heffter

ECHIDNA: A System for Manipulating Explicit Choice Higher Dimensional Automata 587
R. Buckland and M. Johnson

Verification Using PEP 591
S. Melzer, S. Römer, J. Esparza

The FC2TOOLS Set 595
A. Bouali, A. Ressouche, V. Roy, R. de Simone

Programming in Lygon: A System Demonstration 599
J. Harland, D. Pym, M. Winikoff

CtCoq: A System Presentation 600
J. Bertot and Y. Bertot

The TYPELAB Specification and Verification Environment 604
F.W. von Henke, M. Luther, H. Pfeifer, H. Rueß, D. Schwier, M. Strecker, M. Wagner

Incremental Formalization 608
B. Steffen, T. Margaria, A. Claßen, V. Braun

PROPLANE: A Specification Development Environment 612
J. Souquières and N. Lévy

A Logic-Based Technology to Mechanize Software Components Reuse 616
P. Parot

TkGofer: A Functional GUI Library 621
W. Schulte, T. Schwinn, T. Vullinghs

ALPHA - A Class Library for a Metamodel Based on Algebraic Graph Theory 625
S. Erdmann and I. Claßen

Resolution of Goals with the Functional and Logic Programming Language LPG: Impact of Abstract Interpretation 629
D. Bert, R. Echahed, K. Adi

Combining Reductions and Computations in ReDuX 633
R. Bündgen and W. Lauterbach

Conditional Directed Narrowing 637
S. Limet and P. Réty

Author Index 641