Michael Johnson (Ed.)

Algebraic Methodology and Software Technology

6th International Conference, AMAST'97
Sydney, Australia, December 13-17, 1997
Proceedings

Springer

Lecture Notes in Computer Science 1349
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Michael Johnson
Macquarie University
School of Mathematics, Physics, Computing, and Electronics
Sydney NSW 2109, Australia
E-mail: mike@mpce.mq.edu.au

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Algebraic methodology and software technology : 6th international conference ; proceedings / AMAST '97, Sydney, Australia, December 13 - 17, 1997. Michael Johnson (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1997
(Lecture notes in computer science ; Vol. 1349)
ISBN 3-540-63888-1

CR Subject Classification (1991): F3-4, D.2, C.3, D.1.6, I.2.3, H.2.1-4

ISSN 0302-9743
ISBN 3-540-63888-1 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 1997
Printed in Germany

Typesetting: Camera-ready by author
SPIN 10652702 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

The sixth international Algebraic Methodology and Software Technology Conference (AMAST'97) was held in Sydney, Australia, between December 13 and December 17, 1997. Previous AMAST conferences had been held in Iowa (1989 and 1991), in Twente (1993), in Montreal (1995), and in Munich (1996).

Over the years AMAST has developed into a wide ranging initiative with a number of workshops held each year in addition to the now annual AMAST conference. For me the outstanding feature of AMAST, present again this year, is its mix of serious mathematical development of formal methods in software engineering with practical concerns, tools, case studies, and industrial involvement. The annual conference is a special opportunity for theoreticians, practitioners, and industrial participants to share their experiences in advancing software technology, programming methodology, and their algebraic and logical foundations.

AMAST'97 attracted an unusually large number of submissions resulting in extraordinary workloads for this year's programme committee: V.S. Alagar (Canada), Egidio Astesiano (Italy), Didier Begay (France), R. Buckland (Australia), J. Cannon (Australia), Kokichi Futatsugi (Japan), Armando Haeberer (Brazil), Paola Inverardi (Italy), Michael Johnson (Australia), Rocco De Nicola (Italy), Anton Nijholt (Holland), Fernando Orejas (Spain), Mehmet Orgun (Australia), John Plaice (Australia) John Potter (Australia),R. Ramanujam (India), Charles Rattray (Great Britain), T. Rus (USA), T. Sakabe (Japan), Giuseppe Scollo (Holland), R.K. Shyamasundar (India), Andrzej Tarlecki (Poland), R.F.C. Walters (Australia), and M. Wirsing (Germany).

The programme committee also needed to call on a large number of additional referees including: A. Arnold, Marek Bednarczyk, Michele Boreale, Tomasz Borzyszkowski, Pietro Cenciarelli, Maura Cerioli, Corina Cirstea, Flavio Corradini, Eva Coscia, Maarten Fokkinga, Thom Fruehwirth, Stefania Gnesi, James Harland, A.W. Heerink, David Janin, Joost-Pieter Katoen, Alexander Knapp, Anton Koelbl, Beata Konikowska, Anna Labella, Diego Latella, Huimin Lin, Chuchang Liu, Kamal Lodaya, P. Madhusudan, Alfio Martini, Scott McCallum, Chiara Meo, Stephan Merz, Ugo Montanari, Carlo Montangero, Madhavan Mukund, Tohru Naoi, K. Narayan Kumar, Monica Nesi, Geoff Outhred, Catuscia Palamidessi, Paritosh Pandya, Joachim Parrow, Mannes Poel, Corrado Priami, Rosario Pugliese, N. Raja, Gianna Reggio, Bernhard Reus, Michael Richmond, Ken Robinson, Robert Rosebrugh, Igor Shparlinski, G. Sivakumar, Masahiko Skai, P.S. Subramanian, Pim van den Broek, Axel Wabenhorst, Uwe Wolter, Shinichirou Yamamoto, Shoji Yuen, Xiaogang Zhang, Elena Zucca, Job Zwiers.

The systems and tools demonstrations committee was chaired by Richard Buckland and consisted of Richard Buckland, Ken Robinson, and Jon Tidswell. Local arrangements were coordinated by Vicki Carruthers.

The organisers are grateful for the support of Macquarie University and its Department of Computing, the Microsoft Research Institute, the Joint Research Centre for Advanced Systems Engineering and the Australian Research Council.

October 1997 Michael Johnson

Table of Contents

Software configuration with information systems
by *Slim Ben Lamine and John Plaice* 1

Head-tactics simplification
by *Yves Bertot* 16

Iteration 2-theories
by *Stephen L. Bloom, Zoltán Ésik, Anna Labella and Ernest G. Manes* 30

Model checking and fault tolerance
by *Glenn Bruns and Ian Sutherland* 45

Deadlock analysis for a fault-tolerant system
by *Bettina Buth, Michel Kouvaras, Jan Peleska and Hui Shi* 60

From sequential to multi-threaded Java: An event-based operational semantics
by *Pietro Cenciarelli, Alexander Knapp, Bernhard Reus and Martin Wirsing* 75

Permissive subsorted partial logic in CASL
by *Maura Cerioli, Anne Haxthausen, Bernd Krieg-Brückner and Till Mossakowski* 91

Specification of timing constraints within the Circal process algebra
by *Antonio Cerone and George J. Milne* 108

On the specification and verification of performance properties for a timed process algebra
by *Xiao Jun Chen and Flavio Corradini* 123

Abstract interpretation of algebraic polynomial systems
by *Patrick Cousot and Radhia Cousot* 138

Modular refinement and model building
by *Martin de Groot and Ken Robinson* 155

A linear temporal logic approach to objects with transactions
by *Grit Denker, Jaime Ramos, Carlos Caleiro and Amílcar Sernadas* 170

Software design, specification, and verification: Lessons learned from the Rether case study
by *Xiaoqun Du, Kevin T. McDonnell, Evangelos Nanos, Y.S. Ramakrishna and Scott A. Smolka* 185

Refinement rules for real-time multi-tasking programs
by *C.J. Fidge* 199

Rigorous object oriented-modeling: Integrating formal and informal notations
by *R.B. France, J.-M. Bruel, M.M. Larrondo-Petrie and E. Grant* . . 216

Completeness in abstract interpretation: A domain perspective
by *Roberto Giacobazzi and Francesco Ranzato* 231

Floating point verification in HOL Light: The exponential function
by *John Harrison* 246

Verification of distributed real-time and fault-tolerant protocols
by *Jozef Hooman* 261

Invariants, bisimulations and the correctness of coalgebraic refinements
by *Bart Jacobs* 276

On bisimulation, fault-monotonicity and provable fault-tolerance
by *Tomasz Janowski* 292

Span(Graph): A categorical algebra of transition systems
by *Piergiulio Katis, N. Sabadini and R.F.C. Walters* 307

Representing place/transition nets in Span(Graph)
by *Piergiulio Katis, N. Sabadini and R.F.C. Walters* 322

Invariants of parameterized binary tree networks as greatest fixpoints
by *David Lesens* 337

Modelling specification construction by successive approximations
by *Nicole Lévy and Jeanine Souquières* 351

On partial validation of logic programs
by *Sébastien Limet and Frédéric Saubion* 365

Preservation and reflection in specification
by *A. Lopes and J.L. Fiadeiro* 380

Case studies in using a meta-method for formal method integration
by *Richard F. Paige* 395

The update calculus
by *Joachim Parrow and Björn Victor* 409

Selective attribute elimination for categorical data specifications
by *Frank Piessens and Eric Steegmans* 424

ATM switch design: Parametric high-level modeling and formal verification
by *Sreeranga P. Rajan and Masahiro Fujita* 437

The hidden function question revisited
by *Arno Schönegge* 451

Synchronization of logics with mixed rules: Completeness preservation
by *Amílcar Sernadas, Cristina Sernadas and Carlos Caleiro* 465

Symbolic bisimulation for Full LOTOS
by *Carron Shankland and Muffy Thomas* 479

Algebraic composition and refinement of proofs
by *Martin Simons and Michel Sintzoff* 494

Ensuring streams flow
by *Alastair Telford and David Turner* 509

Extending process languages with time
by *Irek Ulidowski and Shoji Yuen* 524

Parametric analysis of computer systems
by *Farn Wang and Pao-Ann Hsiung* 539

Systems and Tools Demonstrations

CAMILA: Prototyping and refinement of constructive specifications
by *J.J. Almeida, L.S. Barbosa, F.L. Neves and J.N. Oliveira* 554

PAMELA+PVS
by *Bettina Buth* 560

The Circal system
by *Antonio Cerone, Alex J. Cowie and George J. Milne* 563

A refinement-type checker for Standard ML
by *Rowan Davies* 565

Recording HOL proofs in a structured browsable format
by *Jim Grundy and Thomas Långbacka* 567

Analysing multi-agent system traces with IDAF
by *C.K. Low* 572

DOVE: A tool for design oriented verification and evaluation
by *M.A. Ozols, K.A. Eastaughffe and A. Cant* 574

The B Method and the B Toolkit
by *Ken Robinson* 576

An algebraic language processing environment
by *Teodor Rus, Tom Halverson, Eric Van Wyk and Robert Kooima* . 581

The Cogito development system
by *Owen Traynor, Dan Hazel, Peter Kearney, Andrew Martin, Ray Nickson and Luke Wildman* 586

Author Index 593