

Lecture Notes in Computer Science

2030

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

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

Furio Honsell Marino Miculan (Eds.)

Foundations of Software Science and Computation Structures

4th International Conference, FOSSACS 2001
Held as Part of the Joint European Conferences
on Theory and Practice of Software, ETAPS 2001
Genova, Italy, April 2-6, 2001
Proceedings



Springer

Series Editors

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

Volume Editors

Furio Honsell
Marino Miculan
Università di Udine, Dipartimento di Matematica e Informatica
Via delle Scienze 206, 33100 Udine, Italy
E-mail: {honsell/miculan}@dimi.uniud.it

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Foundations of software science and computation structures : 4th international conference ; proceedings / FOSSACS 2001, held as part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2001, Genova, Italy, April 2 - 6, 2001. Furio Honsell ; Marino Miculan (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London Milan ; Paris ; Singapore ; Tokyo : Springer, 2001 (Lecture notes in computer science ; Vol. 2030)
ISBN 3-540-41864-4

CR Subject Classification (1998): F.3, F.4.2, F.1.1, D.3.3-4, D.2.1

ISSN 0302-9743

ISBN 3-540-41864-4 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 New York
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2001
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna
Printed on acid-free paper SPIN: 10782468 06/3142 5 4 3 2 1 0

Foreword

ETAPS 2001 was the fourth instance of the European Joint Conferences on Theory and Practice of Software. ETAPS is an annual federated conference that was established in 1998 by combining a number of existing and new conferences. This year it comprised five conferences (FOSSACS, FASE, ESOP, CC, TACAS), ten satellite workshops (CMCS, ETI Day, JOSES, LDTA, MMAABS, PFM, ReMiS, UNIGRA, WADT, WTUML), seven invited lectures, a debate, and ten tutorials.

The events that comprise ETAPS address various aspects of the system development process, including specification, design, implementation, analysis, and improvement. The languages, methodologies, and tools which support these activities are all well within its scope. Different blends of theory and practice are represented, with an inclination towards theory with a practical motivation on one hand and soundly-based practice on the other. Many of the issues involved in software design apply to systems in general, including hardware systems, and the emphasis on software is not intended to be exclusive.

ETAPS is a loose confederation in which each event retains its own identity, with a separate program committee and independent proceedings. Its format is open-ended, allowing it to grow and evolve as time goes by. Contributed talks and system demonstrations are in synchronized parallel sessions, with invited lectures in plenary sessions. Two of the invited lectures are reserved for “unifying” talks on topics of interest to the whole range of ETAPS attendees. The aim of cramming all this activity into a single one-week meeting is to create a strong magnet for academic and industrial researchers working on topics within its scope, giving them the opportunity to learn about research in related areas, and thereby to foster new and existing links between work in areas that were formerly addressed in separate meetings.

ETAPS 2001 was hosted by the Dipartimento di Informatica e Scienze dell’Informazione (DISI) of the Università di Genova and was organized by the following team:

Egidio Astesiano (General Chair)
Eugenio Moggi (Organization Chair)
Maura Cerioli (Satellite Events Chair)
Gianna Reggio (Publicity Chair)
Davide Ancona
Giorgio Delzanno
Maurizio Martelli

with the assistance of Convention Bureau Genova. Tutorials were organized by Bernhard Rumpe (TU München). Overall planning for ETAPS conferences is the responsibility of the ETAPS Steering Committee, whose current membership is:

Egidio Astesiano (Genova), Ed Brinksma (Enschede), Pierpaolo Degano (Pisa), Hartmut Ehrig (Berlin), José Fiadeiro (Lisbon), Marie-Claude Gaudel (Paris), Susanne Graf (Grenoble), Furio Honsell (Udine), Nigel

Horspool (Victoria), Heinrich Hußmann (Dresden), Paul Klint (Amsterdam), Daniel Le M'etayer (Rennes), Tom Maibaum (London), Tiziana Margaria (Dortmund), Ugo Montanari (Pisa), Mogens Nielsen (Aarhus), Hanne Riis Nielson (Aarhus), Fernando Orejas (Barcelona), Andreas Podelski (Saarbrücken), David Sands (Göteborg), Don Sannella (Edinburgh), Perdita Stevens (Edinburgh), Jerzy Tiuryn (Warsaw), David Watt (Glasgow), Herbert Weber (Berlin), Reinhard Wilhelm (Saarbrücken)

ETAPS 2001 was organized in cooperation with

the Association for Computing Machinery
the European Association for Programming Languages and Systems
the European Association of Software Science and Technology
the European Association for Theoretical Computer Science

and received generous sponsorship from:

ELSAG
Fondazione Cassa di Risparmio di Genova e Imperia
INDAM – Gruppo Nazionale per l'Informatica Matematica (GNIM)
Marconi
Microsoft Research
Telecom Italia
TXT e-solutions
Università di Genova

I would like to express my sincere gratitude to all of these people and organizations, the program committee chairs and PC members of the ETAPS conferences, the organizers of the satellite events, the speakers themselves, and finally Springer-Verlag for agreeing to publish the ETAPS proceedings.

January 2001

Donald Sannella
ETAPS Steering Committee chairman

Preface

The present volume contains the proceedings of the international conference *Foundations of Software Science and Computation Structures* (FOSSACS 2001), held in Genova, Italy, April 2-4, 2001. FOSSACS is a constituent event of the *Joint European Conferences on Theory and Practice of Software* (ETAPS). This was the fourth meeting of ETAPS. The previous three meetings took place in Lisbon (1998), Amsterdam (1999), and Berlin (2000).

FOSSACS seeks papers significant to software sciences, which offer progress in foundational research. Central objects of interest are the algebraic, categorical, logical, and geometric theories, models, and methods which support the specification, synthesis, verification, analysis, and transformation of sequential, concurrent, distributed, and mobile programs and software systems. This volume deals with a wide spectrum of topics within this scope, many of which are motivated by recent trends and problems in the practice of software and information technology.

There are 27 papers in these proceedings. The first one accompanies the invited lecture *Adequacy for algebraic effects*, delivered by Gordon Plotkin (Edinburgh University) at FOSSACS 2001. The last one concerns a tool presentation. The other 25 are contributed papers, selected out of a total of 63 submissions. Each paper was thoroughly evaluated by the PC members. The selection procedure ended with a virtual meeting of the Program Committee which lasted over a week. I would like to sincerely thank all of the PC members for the excellent work they did during this difficult process. The tool presentation was selected by a special committee appointed by Donald Sannella the ETAPS Chairman.

Very special thanks go to the co-editor of these proceedings Marino Miculan, whose assistance has been invaluable in organizing the conference web-page, the electronic submission, reviewing, and notification processes, as well as in preparing the files for the publisher. Thanks to Richard van de Stadt for producing and allowing us to utilize the *CyberChair* software. And thanks also to all the members of the Organizing Committee, chaired by Egidio Astesiano, Eugenio Moggi, and Gianna Reggio. Finally I would like to thank the Steering Committee of ETAPS, and especially its Chairman Donald Sannella, for the precious advice and excellent coordination in all the various activities leading up to this FOSSACS conference.

January 2001

Furio Honsell
FOSSACS 2001 Program Committee Chair

FOSSACS 2001 Program Committee

Luca Cardelli (Cambridge, UK)	Furio Honsell (Udine, Italy, chair)
Philippe Darondeau (Rennes, France)	Pierre Lescanne (Lyon, France)
Mariangiola Dezani (Torino, Italy)	Ugo Montanari (Pisa, Italy)
Abbas Edalat (London, UK)	Mogens Nielsen (Århus, Denmark)
Javier Esparza (München, Germany)	Mitsu Okada (Tokyo, Japan)
Bart Jacobs (Nijmegen, The Netherlands)	Carolyn Talcott (Stanford, USA)
Matthew Hennessy (Sussex, UK)	Pawel Urzyczyn (Warsaw, Poland)
Martin Hofmann (Edinburgh, UK)	Igor Walukiewicz (Warsaw, Poland)

List of Referees

Fabio Alessi	Catalin Dima
Roberto Amadio	Dan Dougherty
Andre Arnold	Gilles Dowek
Paolo Baldan	Hartmut Ehrig
Stefano Berardi	Thomas Engel
Marco Bernardo	Alessandro Fantechi
Richard Blute	Maribel Fernandez
Chiara Bodei	Paolo Ferragina
Mikolaj Bojanczyk	Andrzej Filinski
Marcello Bonsangue	Marcelo Fiore
Ahmed Bouajjani	Cedric Fournet
Jérémie Bourdon	Massimo Franceschet
Julian Bradfield	Carsten Führmann
Roberto Bruni	Maurizio Gabbrielli
Nadia Busi	Philippa Gardner
Benoit Caillaud	Paul Gastin
Olivier Carton	Stephane Gaubert
Paul Caspi	Paola Giannini
Ilaria Castellani	Juergen Giesl
Jan Cederquist	Stefania Gnesi
Jacek Chrzaszcz	Andrew D. Gordon
Paolo Ciancarini	Bernd Grobauer
David Clark	Josef Gruska
Hubert Comon	Stefano Guerrini
Adriana Compagnoni	Jesper Gulmann Henriksen
Mario Coppo	Vineet Gupta
Andrea Corradini	Masahito Hasegawa
Rocco De Nicola	Reiko Heckel
Philippe Devienne	Reinhold Heckmann
Fer-Jan de Vries	Keijo Heljanko
Pietro Di Gianantonio	Hugo Herbelin
Krzysztof Diks	Holger Hermanns

Daniel Hirschkoff
 Ian Hodkinson
 Markus Holzer
 Thomas Hune
 Graham Hutton
 Katsushi Inoue
 Radha Jagadeesan
 David Janin
 Marcin Jurdzinski
 Richard Kennaway
 Delia Kesner
 Astrid Kiehn
 Dilsun Kirli
 Teodor Knapik
 Barbara Koenig
 Antonin Kucera
 Ralf Kuesters
 Alexander Kurz
 Dietrich Kuske
 Marta Kwiatkowska
 Slawomir Lasota
 Marina Lenisa
 Francesca Levi
 Luigi Liquori
 Gerald Luetzgen
 Angelika Mader
 Pasquale Malacaria
 Narciso Marti-Oliet
 Michael Marz
 Richard Mayr
 Guy McCusker
 Massimo Merro
 Marino Miculan
 Angelo Montanari
 César A. Muñoz H.
 Anca Muscholl
 Margherita Napoli
 Mirabelle Nebut
 Mitsuhiro Okada
 Joachim Parrow
 Christine Paulin-Mohring
 Larry C. Paulson
 Wieslaw Pawlowski
 Adriano Peron
 Carla Piazza
 Sophie Pinchinat

Erik Poll
 John Power
 K. V. S. Prasad
 Rosario Pugliese
 R. Ramanujam
 Jean-Xavier Rampon
 Julian Rathke
 Bernhard Reus
 Eike Ritter
 Simona Ronchi Della Rocca
 Francesca Rossi
 Luca Roversi
 Ivano Salvo
 Don Sannella
 Luigi Santocanale
 Vladimiro Sassone
 Ivan Scagnetto
 Aleksy Schubert
 Francesca Scozzari
 Peter Selinger
 Paula Severi
 Jiří Srba
 Alin Stefanescu
 Perdita Stevens
 Makoto Takeyama
 Francis Tang
 Hendrik Tews
 Wolfgang Thomas
 Simone Tini
 Yoshihito Toyama
 Daniele Turi
 Tomasz Urbanski
 Frank Valencia
 Andrea Valente
 Daniele Varacca
 Betti Venneri
 Marisa Venturini Zilli
 Rene Vestergaard
 Alicia Villanueva
 Daria Walukiewicz
 Freek Wiedijk
 Nobuko Yoshida
 Hans Zantema
 Pascal Zimmer
 Jan Zwanenburg

Table of Contents

Invited Paper

Adequacy for Algebraic Effects	1
<i>Gordon Plotkin and John Power</i>	

Contributed Papers

Secrecy Types for Asymmetric Communication	25
<i>Martín Abadi and Bruno Blanchet</i>	
Axiomatizing Tropical Semirings.....	42
<i>Luca Aceto, Zoltán Ésik, and Anna Ingólfssdóttir</i>	
Type Isomorphisms and Proof Reuse in Dependent Type Theory	57
<i>Gilles Barthe and Olivier Pons</i>	
On the Duality between Observability and Reachability.....	72
<i>Michel Bidoit, Rolf Hennicker, and Alexander Kurz</i>	
The Finite Graph Problem for Two-Way Alternating Automata.....	88
<i>Mikołaj Bojańczyk</i>	
High-Level Petri Nets as Type Theories in the Join Calculus.....	104
<i>Maria Grazia Buscemi and Vladimiro Sassone</i>	
Temporary Data in Shared Dataspace Coordination Languages	121
<i>Nadia Busi, Roberto Gorrieri, and Gianluigi Zavattaro</i>	
On Garbage and Program Logic.....	137
<i>Cristiano Calcagno and Peter W. O’Hearn</i>	
The Complexity of Model Checking Mobile Ambients.....	152
<i>Witold Charatonik, Silvano Dal Zilio, Andrew D. Gordon, Supratik Mukhopadhyay, and Jean-Marc Talbot</i>	
The Rho Cube	168
<i>Horatiu Cirstea, Claude Kirchner, and Luigi Liquori</i>	
Type Inference with Recursive Type Equations.....	184
<i>Mario Coppo</i>	
On the Modularity of Deciding Call-by-Need	199
<i>Irène Durand and Aart Middeldorp</i>	
Synchronized Tree Languages Revisited and New Applications.....	214
<i>Valérie Gouranton, Pierre Réty, and Helmut Seidl</i>	

Computational Completeness of Programming Languages Based on Graph Transformation	230
<i>Annegret Habel and Detlef Plump</i>	
Axioms for Recursion in Call-by-Value (Extended Abstract)	246
<i>Masahito Hasegawa and Yoshihiko Kakutani</i>	
Class Analysis of Object-Oriented Programs through Abstract Interpretation	261
<i>Thomas Jensen and Fausto Spoto</i>	
On the Complexity of Parity Word Automata	276
<i>Valerie King, Orna Kupferman, and Moshe Y. Vardi</i>	
Foundations for a Graph-Based Approach to the Specification of Access Control Policies	287
<i>Manuel Koch, Luigi Vincenzo Mancini, and Francesco Parisi-Presicce</i>	
Categories of Processes Enriched in Final Coalgebras	303
<i>Sava Krstić, John Launchbury, and Duško Pavlović</i>	
Model Checking CTL ⁺ and FCTL Is Hard	318
<i>François Laroussinie, Nicolas Markey, and Philippe Schnoebelen</i>	
On Regular Message Sequence Chart Languages and Relationships to Mazurkiewicz Trace Theory	332
<i>Rémi Morin</i>	
Verified Bytecode Verifiers	347
<i>Tobias Nipkow</i>	
Higher-Order Abstract Syntax with Induction in Isabelle/HOL: Formalizing the π -Calculus and Mechanizing the Theory of Contexts	364
<i>Christine Röckl, Daniel Hirschhoff, and Stefan Berghofer</i>	
Decidability of Weak Bisimilarity for a Subset of Basic Parallel Processes ..	379
<i>Colin Stirling</i>	
An Axiomatic Semantics for the Synchronous Language <i>Gentzen</i>	394
<i>Simone Tini</i>	

Tool Presentation

MARRELLA and the Verification of an Embedded System	409
<i>Dominique Ambroise, Patrick Augé, Kamel Bouchefra, and Brigitte Rozoy</i>	
Author Index	413