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
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, RelMiS, 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
VI Foreword

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 (Arhus, 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
Table of Contents

Invited Paper
Adequacy for Algebraic Effects .............................................. 1
   Gordon Plotkin and John Power

Contributed Papers
Secrecy Types for Asymmetric Communication ......................... 25
   Martín Abadi and Bruno Blanchet

Axiomatizing Tropical Semirings ........................................... 42
   Luca Aceto, Zoltán Ésik, and Anna Ingólfsdóttir

Type Isomorphisms and Proof Reuse in Dependent Type Theory ........ 57
   Gilles Barthe and Olivier Pons

On the Duality between Observability and Reachability .............. 72
   Michel Bidoit, Rolf Hennicker, and Alexander Kurz

The Finite Graph Problem for Two-Way Alternating Automata .......... 88
   Mikołaj Bojańczyk

High-Level Petri Nets as Type Theories in the Join Calculus .......... 104
   Maria Grazia Buscemi and Vladimiro Sassone

Temporary Data in Shared Dataspace Coordination Languages .......... 121
   Nadia Busi, Roberto Gorrieri, and Gianluigi Zavattaro

On Garbage and Program Logic ............................................. 137
   Cristiano Calcagno and Peter W. O'Hearn

The Complexity of Model Checking Mobile Ambients .................... 152
   Witold Charatonik, Silvano Dal Zilio, Andrew D. Gordon,
   Supratik Mukhopadhyay, and Jean-Marc Talbot

The Rho Cube ......................................................................... 168
   Horatiu Cirstea, Claude Kirchner, and Luigi Liquori

Type Inference with Recursive Type Equations .......................... 184
   Mario Coppo

On the Modularity of Deciding Call-by-Need .............................. 199
   Irène Durand and Aart Middeldorp

Synchronized Tree Languages Revisited and New Applications ........ 214
   Valérie Gouranton, Pierre Réty, and Helmut Seidl
Computational Completeness of Programming Languages Based on Graph Transformation ............................................................ 230
    Annegret Habel and Detlef Plump

Axioms for Recursion in Call-by-Value (Extended Abstract) .................. 246
    Masahito Hasegawa and Yoshihiko Kakutani

Class Analysis of Object-Oriented Programs through Abstract Interpretation ............................................................. 261
    Thomas Jensen and Fausto Spoto

On the Complexity of Parity Word Automata ................................. 276
    Valerie King, Orna Kupferman, and Moshe Y. Vardi

Foundations for a Graph-Based Approach to the Specification of Access Control Policies ...................................................... 287
    Manuel Koch, Luigi Vincenzo Mancini, and Francesco Parisi-Presicce

Categories of Processes Enriched in Final Coalgebras ...................... 303
    Sava Krstić, John Launchbury, and Duško Pavlović

Model Checking CTL+ and FCTL Is Hard ................................318
    François Laroussinie, Nicolas Markey, and Philippe Schnoebelen

On Regular Message Sequence Chart Languages and Relationships to Mazurkiewicz Trace Theory ............................................... 332
    Rémi Morin

Verified Bytecode Verifiers.................................................347
    Tobias Nipkow

Higher-Order Abstract Syntax with Induction in Isabelle/HOL:
Formalizing the π-Calculus and Mechanizing the Theory of Contexts ...... 364
    Christine Röckl, Daniel Hirschkoff, and Stefan Berghofer

Decidability of Weak Bisimilarity for a Subset of Basic Parallel Processes . 379
    Colin Stirling

An Axiomatic Semantics for the Synchronous Language Gentzen.........394
    Simone Tini

Tool Presentation

MARRELLA and the Verification of an Embedded System .................. 409
    Dominique Ambroise, Patrick Augé, Kamel Bouchezra, and Brigitte Rozoy

Author Index .......................................................... 413