

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Alfred Kobsa

*University of California, Irvine, CA, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*University of Dortmund, Germany*

Madhu Sudan

*Massachusetts Institute of Technology, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

Luca de Alfaro (Ed.)

# Foundations of Software Science and Computational Structures

12th International Conference, FOSSACS 2009  
Held as Part of the Joint European Conferences  
on Theory and Practice of Software, ETAPS 2009  
York, UK, March 22-29, 2009  
Proceedings

## Volume Editor

Luca de Alfaro  
University of California  
School of Engineering  
Dept. of Computer Engineering  
1156 High Street MS: SOE3, Santa Cruz, CA 95064, USA  
E-mail: luca@soe.ucsc.edu

Library of Congress Control Number: 2009922287

CR Subject Classification (1998): F.3, F.1, F.4, D.3, D.2

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743  
ISBN-10 3-642-00595-0 Springer Berlin Heidelberg New York  
ISBN-13 978-3-642-00595-4 Springer 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. Violations are liable to prosecution under the German Copyright Law.

springer.com

© Springer-Verlag Berlin Heidelberg 2009  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper SPIN: 12632343 06/3180 5 4 3 2 1 0

# Foreword

ETAPS 2009 was the 12th 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 (CC, ESOP, FASE, FOSSACS, TACAS), 22 satellite workshops (ACCAT, ARSPA-WITS, Bytecode, COCV, COMPASS, FESCA, FInCo, FORMED, GaLoP, GT-VMT, HFL, LDTA, MBT, MLQA, OpenCert, PLACES, QAPL, RC, SafeCert, TAASN, TERMGRAPH, and WING), four tutorials, and seven invited lectures (excluding those that were specific to the satellite events). The five main conferences received 532 submissions (including 30 tool demonstration papers), 141 of which were accepted (10 tool demos), giving an overall acceptance rate of about 26%, with most of the conferences at around 25%. Congratulations therefore to all the authors who made it to the final programme! I hope that most of the other authors will still have found a way of participating in this exciting event, and that you will all continue submitting to ETAPS and contributing towards making it the best conference on software science and engineering.

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 the 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 confederation in which each event retains its own identity, with a separate Programme Committee and proceedings. Its format is open-ended, allowing it to grow and evolve as time goes by. Contributed talks and system demonstrations are in synchronised 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 2009 was organised by the University of York in cooperation with

- ▷ European Association for Theoretical Computer Science (EATCS)
- ▷ European Association for Programming Languages and Systems (EAPLS)
- ▷ European Association of Software Science and Technology (EASST)

and with support from ERCIM, Microsoft Research, Rolls-Royce, Transitive, and Yorkshire Forward.

The organising team comprised:

|                  |                                     |
|------------------|-------------------------------------|
| Chair            | Gerald Luetzgen                     |
| Secretariat      | Ginny Wilson and Bob French         |
| Finances         | Alan Wood                           |
| Satellite Events | Jeremy Jacob and Simon O'Keefe      |
| Publicity        | Colin Runciman and Richard Paige    |
| Website          | Fiona Polack and Malihe Tabatabaie. |

Overall planning for ETAPS conferences is the responsibility of its Steering Committee, whose current membership is:

Vladimiro Sassone (Southampton, Chair), Luca de Alfaro (Santa Cruz), Roberto Amadio (Paris), Giuseppe Castagna (Paris), Marsha Chechik (Toronto), Sophia Drossopoulou (London), Hartmut Ehrig (Berlin), Javier Esparza (Munich), Jose Fiadeiro (Leicester), Andrew Gordon (MSR Cambridge), Rajiv Gupta (Arizona), Chris Hankin (London), Laurie Hendren (McGill), Mike Hinchey (NASA Goddard), Paola Inverardi (L'Aquila), Joost-Pieter Katoen (Aachen), Paul Klint (Amsterdam), Stefan Kowalewski (Aachen), Shriram Krishnamurthi (Brown), Kim Larsen (Aalborg), Gerald Luetzgen (York), Rupak Majumdar (Los Angeles), Tiziana Margaria (Göttingen), Ugo Montanari (Pisa), Oege de Moor (Oxford), Luke Ong (Oxford), Catuscia Palamidessi (Paris), George Papadopoulos (Cyprus), Anna Philippou (Cyprus), David Rosenblum (London), Don Sannella (Edinburgh), João Saraiva (Minho), Michael Schwartzbach (Aarhus), Perdita Stevens (Edinburgh), Gabriel Taentzer (Marburg), Dániel Varró (Budapest), and Martin Wirsing (Munich).

I would like to express my sincere gratitude to all of these people and organisations, the Programme Committee Chairs and PC members of the ETAPS conferences, the organisers of the satellite events, the speakers themselves, the many reviewers, and Springer for agreeing to publish the ETAPS proceedings. Finally, I would like to thank the Organising Chair of ETAPS 2009, Gerald Luetzgen, for arranging for us to hold ETAPS in the most beautiful city of York.

January 2009

Vladimiro Sassone, Chair  
ETAPS Steering Committee

# Preface

The present volume contains the proceedings of the 12th International Conference on the Foundations of Software Science and Computations Structures (FOSSACS) 2009, held in York, UK, March 22-25, 2009. FOSSACS is an event of the Joint European Conferences on Theory and Practice of Software (ETAPS). The previous 11 FOSSACS conferences took place in Lisbon (1998), Amsterdam (1999), Berlin (2000), Genoa (2001), Grenoble (2002), Warsaw (2003), Barcelona (2004), Edinburgh (2005), Vienna (2006), Braga (2007), and Budapest (2008).

FOSSACS presents original papers on foundational research with a clear significance to software science. The Programme Committee (PC) invited submissions on theories and methods to support analysis, synthesis, transformation and verification of programs and software systems.

This proceedings volume contains 30 regular papers, as well as the abstracts of two invited talks. The first invited talk, “Temporal Reasoning About Program Executions”, was by Rajeev Alur, the FOSSACS 2009 invited speaker. The second invited talk, “Facets of Synthesis: Revisiting Church’s Problem”, was by Wolfgang Thomas, one of the two unifying ETAPS 2009 invited speakers.

We received 122 abstracts and 102 full paper submissions; of these, 30 were selected for presentation at FOSSACS and inclusion in the proceedings. The selection process was performed by the PC in the course of a two-week electronic meeting. The PC members, and the external experts they consulted, wrote a total of over 400 paper reviews, and the discussion phase of the meeting involved several hundred messages. I was very impressed by the work done by the PC members, and by the external experts, both before and during the PC meeting. The competition was particularly fierce, and many good papers could not be accepted.

We sincerely thank all the authors of papers submitted to FOSSACS 2009. Moreover, we would like to thank the members of the PC for their excellent job during the selection process, as well as all the sub-reviewers for the expert help and reviews they provided. Through the phases of submission, evaluation, and production of the proceedings we relied on the invaluable assistance of the EasyChair system; we are very grateful to its developer Andrei Voronkov, and to all its maintainers. Last but not least, we would like to thank the ETAPS 2009 Organizing Committee chaired by Gerald Luetzgen and the ETAPS Steering Committee chaired by Vladimiro Sassone for their efficient coordination of all the activities leading up to FOSSACS 2009.

# Conference Organization

## Programme Chair

Luca de Alfaro

## Programme Committee

|                        |   |
|------------------------|---|
| Parosh Abdulla         | Uppsala University                      |
| Roberto Amadio         | Paris Diderot University                |
| Jos Baeten             | Eindhoven University of Technology      |
| Luís Caires            | New University of Lisbon                |
| Luca de Alfaro (Chair) | UC Santa Cruz and Google                |
| Javier Esparza         | Technical University of Munich          |
| Kousha Etessami        | University of Edinburgh                 |
| Marcelo Fiore          | University of Cambridge                 |
| Cédric Fournet         | Microsoft Research                      |
| Dan Ghica              | University of Birmingham                |
| Radha Jagadeesan       | DePaul University                       |
| Alan Jeffrey           | Bell Labs                               |
| Marcin Jurdziński      | University of Warwick                   |
| Naoki Kobayashi        | Tohoku University                       |
| Barbara König          | University of Duisburg-Essen            |
| Ugo Montanari          | University of Pisa                      |
| Catuscia Palamidessi   | INRIA and École Polytechnique           |
| Prakash Panangaden     | McGill University                       |
| Amir Pnueli            | New York University                     |
| Jean-François Raskin   | University of Brussels (ULB)            |
| Grigore Rosu           | University of Illinois Urbana-Champaign |
| Davide Sangiorgi       | University of Bologna                   |
| Carolyn Talcott        | SRI International                       |

## External Reviewers

|                    |                       |
|--------------------|-----------------------|
| Suzana Andova      | Nathalie Bertrand     |
| Jesus Aranda       | Karthikeyan Bhargavan |
| Eugene Asarin      | Stefano Bistarelli    |
| Philippe Audebaud  | Simon Bliudze         |
| Gergei Bana        | Filippo Bonchi        |
| Massimo Bartoletti | Michele Boreale       |
| Josh Berdine       | Richard Bornat        |
| Martin Berger      | Artur Boronat         |

Patricia Bouyer  
Tomas Brazdil  
Franck van Breugel  
Thomas Brihaye  
Sander H.J. Bruggink  
Roberto Bruni  
Mikkel Bundgaard  
Marzia Buscemi  
Zining Cao  
Felice Cardone  
Krishnendu Chatterjee  
Konstantinos Chatzikokolakis  
Feng Chen  
James Cheney  
Yannick Chevalier  
Pierre Clairambault  
Hubert Comon-Lundh  
Brendan Cordy  
Ricardo Corin  
Andrea Corradini  
Véronique Cortier  
Pieter Cuijpers  
Deepak D'Souza  
Arnaud da Costa  
Vincent Danos  
Stéphanie Delaune  
Stéphane Demri  
Josée Desharnais  
Dino Distefano  
Laurent Doyen  
Steven Eker  
Constantin Enea  
Zoltan Esik  
Marco Faella  
John Fearnley  
Jerome Feret  
Gianluigi Ferrari  
Carla Ferreira  
Andrzej Filinski  
Emmanuel Filiot  
Riccardo Focardi  
Wan Fokkink  
Luca Fossati  
Sibylle Froeschle  
David de Frutos-Escrig

Andrew Gacek  
Fabio Gadducci  
Pierre Ganty  
Simon Gay  
Gilles Geeraerts  
Raffaella Gentilini  
Sonja Georgievska  
Giorgio Ghelli  
Sergio Giro  
Gregor Göbller  
Jens Chr. Godsken  
Andy Gordon  
Alexey Gotsman  
Jean Goubault-Larrecq  
Davide Grohmann  
Serge Haddad  
Esfandiar Haghverdi  
Jerry den Hartog  
Masahito Hasegawa  
Tobias Heindel  
Lukas Holik  
Hans Hüttel  
Atsushi Igarashi  
Kazuhiro Inaba  
Yoshinao Isobe  
Neil Jones  
Raman Kazhamiakin  
Bruce Kapron  
Delia Kesner  
Jeroen Ketema  
Stefan Kiefer  
Vijay Anand Korthikanti  
Pavel Krcaľ  
Jörg Kreiker  
Steve Kremer  
Jean Krivine  
Ralf Kuesters  
Alexander Kurz  
Salvatore La Torre  
James Laird  
Yassine Lakhnech  
Ivan Lanese  
Sławomir Lasota  
Luciano Lavagno  
Ranko Lazić



Jean-Jacques Levy  
Alberto Lluch Lafuente  
Christof Loeding  
Michele Loreti  
Dorel Lucanu  
Denis Lugiez  
Michael Luttenberger  
Bas Lutтик  
Ian Mackie  
Pasquale Malacaria  
Louis Mandel  
Giulio Manzonetto  
Nicolas Markey  
Jasen Markovski  
Ian Mason  
Thierry Massart  
Richard Mayr  
Guy McCusker  
Annabelle McIver  
Massimo Merro  
Antoine Meyer  
Marino Miculan  
Dale Miller  
Yasuhiko Minamide  
Larry Moss  
Till Mossakowski  
Mohammad Reza Mousavi  
Gopalan Nadathur  
Uwe Nestmann  
Zhaozhong Ni  
Koki Nishizawa  
Gethin Norman  
Luke Ong  
Simona Orzan  
Luca Padovani  
Miguel Palomino  
Jochen Pfalzgraf  
Andrew Phillips  
Sylvan Pinsky  
Nir Piterman  
Andrei Popescu  
Rosario Pugliese  
Shaz Qadeer  
Paola Quaglia

António Ravara  
Michel Reniers  
Tamara Rezk  
Noam Rinetzky  
Eike Ritter  
Michal Rutkowski  
Sylvain Salvati  
Alexis Saurin  
Lutz Schröder  
Stefan Schwoon  
Traian Serbanuta  
Olivier Serre  
Natalia Sidorova  
Jakob Grue Simonsen  
Alex Simpson  
Anu Singh  
Scott Smith  
Pawel Sobocinski  
Ian Stark  
Kohei Suenaga  
Eijiro Sumii  
Andrzej Tarlecki  
David Teller  
Paul van Tilburg  
Andrea Turrini  
Nikos Tzevelekos  
Frank Valencia  
Hugo Vieira  
Maria Grazia Vigliotti  
Erik de Vink  
Tomáš Vojnar  
Oskar Wibling  
Thomas Wilke  
Hongseok Yang  
Wang Yi  
Anna Zaks  
Eugen Zalinescu  
Marina Zanella  
Hans Zantema  
Gianluigi Zavattaro  
Sami Zhioua  
Wieslaw Zielonka

# Table of Contents

## Invited Talks

|  |    |
|--|----|
| Facets of Synthesis: Revisiting Church’s Problem . . . . . | 1  |
| <i>Wolfgang Thomas</i>                                     |    |
| Temporal Reasoning about Program Executions . . . . .      | 15 |
| <i>Rajeev Alur</i>   |    |

## Semantics

|  |    |
|--|----|
| Least and Greatest Fixpoints in Game Semantics . . . . .                           | 16 |
| <i>Pierre Clairambault</i>   |    |
| Full Abstraction for Reduced ML . . . . .  | 32 |
| <i>Andrzej S. Murawski and Nikos Tzevelekos</i>                                    |    |
| Logics and Bisimulation Games for Concurrency, Causality and<br>Conflict . . . . . | 48 |
| <i>Julian Gutierrez</i>  |    |

## Logics and Automata

|   |     |
|---|-----|
| Separating Graph Logic from MSO . . . . .   | 63  |
| <i>Timos Antonopoulos and Anuj Dawar</i>  |     |
| On the Completeness of Dynamic Logic . . . . .  | 78  |
| <i>Daniel Leivant</i>   |     |
| Dependency Tree Automata . . . . .  | 92  |
| <i>Colin Stirling</i>   |     |
| On Global Model Checking Trees Generated by Higher-Order Recursion<br>Schemes . . . . . | 107 |
| <i>Christopher Broadbent and Luke Ong</i>   |     |

## Algebras

|  |     |
|--|-----|
| A Kleene Theorem for Polynomial Coalgebras . . . . .       | 122 |
| <i>Marcello Bonsangue, Jan Rutten, and Alexandra Silva</i> |     |
| Coalgebraic Hybrid Logic . . . . .                         | 137 |
| <i>Rob Myers, Dirk Pattinson, and Lutz Schröder</i>        |     |

A Description of Iterative Reflections of Monads  
 (Extended Abstract) ..... 152  
*Jiří Adámek, Stefan Milius, and Jiří Velebil*

**Automata Theory**

Tighter Bounds for the Determinisation of Büchi Automata ..... 167  
*Sven Schewe*

Lower Bounds on Witnesses for Nonemptiness of Universal Co-Büchi  
 Automata ..... 182  
*Orna Kupferman and Nir Piterman*

Interrupt Timed Automata ..... 197  
*Beatrice Bérard and Serge Haddad*

Parameter Reduction in Grammar-Compressed Trees ..... 212  
*Markus Lohrey, Sebastian Maneth, and Manfred Schmidt-Schauß*

**Processes and Models**

The Calculus of Handshake Configurations ..... 227  
*Luca Fossati and Daniele Varacca*

On the Expressive Power of Restriction and Priorities in CCS with  
 Replication ..... 242  
*Jesús Aranda, Frank D. Valencia, and Cristian Versari*

Normal Bisimulations in Calculi with Passivation ..... 257  
*Sergueï Lenglet, Alan Schmitt, and Jean-Bernard Stefani*

Reactive Systems, Barbed Semantics, and the Mobile Ambients ..... 272  
*Filippo Bonchi, Fabio Gadducci, and Giacomina Valentina Monreale*

**Security**

On the Foundations of Quantitative Information Flow ..... 288  
*Geoffrey Smith*

Cryptographic Protocol Composition via the Authentication Tests ..... 303  
*Joshua D. Guttman*

Bisimulation for Demonic Schedulers ..... 318  
*Konstantinos Chatzikokolakis, Gethin Norman, and David Parker*

## Probabilistic and Quantitative Models

|   |     |
|---|-----|
| On Omega-Languages Defined by Mean-Payoff Conditions . . . . .                | 333 |
| <i>Rajeev Alur, Aldric Degorre, Oded Maler, and Gera Weiss</i>                |     |
| Minimal Cost Reachability/Coverability in Priced Timed Petri Nets . . . .     | 348 |
| <i>Parosh Aziz Abdulla and Richard Mayr</i>                                   |     |
| Delayed Nondeterminism in Continuous-Time Markov Decision Processes . . . . . | 364 |
| <i>Martin R. Neuhäuser, Mariëlle Stoelinga, and Joost-Pieter Katoen</i>       |     |
| Concurrency, $\sigma$ -Algebras, and Probabilistic Fairness . . . . .         | 380 |
| <i>Samy Abbes and Albert Benveniste</i>                                       |     |

## Synthesis

|  |     |
|--|-----|
| Synthesis from Component Libraries . . . . .                       | 395 |
| <i>Yoad Lustig and Moshe Y. Vardi</i>                              |     |
| Realizability of Concurrent Recursive Programs . . . . .           | 410 |
| <i>Benedikt Bollig, Manuela-Lidia Grindei, and Peter Habermehl</i> |     |

## Program Analysis and Semantics

|   |     |
|---|-----|
| Beyond Shapes: Lists with Ordered Data . . . . .  | 425 |
| <i>Kshitij Bansal, Rémi Brochenin, and Etienne Lozes</i>  |     |
| Interprocedural Dataflow Analysis over Weight Domains with Infinite Descending Chains . . . . .       | 440 |
| <i>Morten Kühnrich, Stefan Schwoon, Jiří Srba, and Stefan Kiefer</i>                                  |     |
| Realizability Semantics of Parametric Polymorphism, General References, and Recursive Types . . . . . | 456 |
| <i>Lars Birkedal, Kristian Størving, and Jacob Thamsborg</i>  |     |

|                               |     |
|-------------------------------|-----|
| <b>Author Index</b> . . . . . | 471 |
|-------------------------------|-----|