

*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*

Sophia Drossopoulou (Ed.)

# Programming Languages and Systems

17th European Symposium on Programming, ESOP 2008  
Held as Part of the Joint European Conferences  
on Theory and Practice of Software, ETAPS 2008  
Budapest, Hungary, March 29-April 6, 2008  
Proceedings



Springer

## Volume Editor

Sophia Drossopoulou  
Imperial College London  
Department of Computing  
SW7 2BZ London, UK  
E-mail: S.Drossopoulou@imperial.ac.uk

Library of Congress Control Number: 2008923060

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

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

ISSN	0302-9743
ISBN-10	3-540-78738-0 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-78738-9 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 is a part of Springer Science+Business Media

[springer.com](http://springer.com)

© Springer-Verlag Berlin Heidelberg 2008  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper      SPIN: 12244515      06/3180      5 4 3 2 1 0

# Foreword

ETAPS 2008 was the 11th 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, AVIS, Bytecode, CMCS, COCV, DCC, FESCA, FIT, FORMED, GaLoP, GT-VMT, LDTA, MBT, MOMPES, PDMC, QAPL, RV, SafeCert, SC, SLA++P, WGT, and WRLA), nine tutorials, and seven invited lectures (excluding those that were specific to the satellite events). The five main conferences received 571 submissions, 147 of which were accepted, giving an overall acceptance rate of less than 26%, with each conference below 27%. 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 to make of it the best conference in the area.

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 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 2008 was organized by the John von Neumann Computer Society jointly with the Budapest University of Technology and the Eötvös University, 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 Microsoft Research and Danubius Hotels.

The organizing team comprised:

Chair	Dániel Varró
Director of Organization	István Alföldi
Main Organizers	Andrea Tósoky, Gabriella Aranyos
Publicity	Joost-Pieter Katoen
Advisors	András Pataricza, João Saraiva
Satellite Events	Zoltán Horváth, Tihamér Levendovszky, Viktória Zsók
Tutorials	László Lengyel
Web Site	Ákos Horváth
Registration System	Victor Francisco Fonte, Zsolt Berényi, Róbert Kereskényi, Zoltán Fodor
Computer Support	Áron Sisak
Local Arrangements	László Gönczy, Gábor Huszerl, Melinda Magyar, several student volunteers.

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), Matt Dwyer (Nebraska), Hartmut Ehrig (Berlin), Chris Hankin (London), Laurie Hendren (McGill), Mike Hinchey (NASA Goddard), Paola Inverardi (L'Aquila), Joost-Pieter Katoen (Aachen), Paul Klint (Amsterdam), Kim Larsen (Aalborg), Gerald Luetzgen (York), Tiziana Margaria (Göttingen), Ugo Montanari (Pisa), Martin Odersky (Lausanne), Catuscia Palamidessi (Paris), Anna Philippou (Cyprus), CR Ramakrishnan (Stony Brook), Don Sannella (Edinburgh), João Saraiva (Minho), Michael Schwartzbach (Aarhus), Helmut Seidl (Munich), Perdita Stevens (Edinburgh), and Dániel Varró (Budapest).

I would like to express my sincere gratitude to all of these people and organizations, the Programme Committee Chairs and members of the ETAPS conferences, the organizers 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 Organizing Chair of ETAPS 2008, Dániel Varró, for arranging for us to have ETAPS in the most beautiful city of Budapest

# Preface

It is an honour to be writing the preface of this volume, containing the papers presented at the 17<sup>th</sup> European Symposium on Programming (ESOP 2008), which took place in Budapest, March 31–April 2, 2008. ESOP is an annual conference devoted to fundamental issues in the specification, analysis, and implementation of programming languages and systems.

This year, ESOP received 104 full submissions out of 136 preliminary submissions. For each submission, at least 3, and on average 3.6, reviews were written. After an intensive electronic meeting (minimizing our carbon footprint) over 4 weeks, the programme committee decided to accept 27 papers, 2 of which are tool presentations.

This volume also contains a summary of the ETAPS invited talk, *Verification of Higher-Order Computation: A Game-Semantic Approach*, given by Luke Ong, and an abstract of the ESOP invited talk, *Constructive Mathematics and Functional Programming*, given by Thierry Coquand.

The papers are listed in the chronological order of their presentation followed by the index of authors.

Thanks go to the authors of all the submitted papers, and to the external referees, who helped us with their excellent reviews. Very many thanks go to the program committee members, for their hard work during the reviewing and the dedicated debates during the selection process.

I am grateful to the EasyChair team for their tool, which provided robust support to all administrative sides of my task.

January 2008

Sophia Drossopoulou

# Conference Organization

## Programme Committee

Davide Ancona	University of Genova, Italy
Manuel Chakravarty	University of New South Wales, Australia
Dave Clarke	CWI, Netherlands
Adriana Compagnoni	Stevens Institute of Technology, USA
Sophia Drossopoulou	Imperial College London, UK
Manuel Fahndrich	Microsoft Research Redmond, USA
Sabine Glesner	Technical University of Berlin, Germany
Robert Harper	Carnegie Mellon University, USA
Shriram Krishnamurthi	Brown University, USA
Doug Lea	State University of New York at Oswego, USA
Alan Mycroft	University of Cambridge, UK
Peter Müller	ETH Zurich, Switzerland and Microsoft Research, USA
David Naumann	Stevens Institute of Technology, USA
Catuscia Palamidessi	INRIA and Ecole Polytechnique, France
Matthew Parkinson	University of Cambridge, UK
German Puebla	Technical University of Madrid, Spain
Andrei Sabelfeld	Chalmers University of Technology, Sweden
Konstantinos Sagonas	National Technical University of Athens, Greece
Vijay Saraswat	Penn State University and IBM T.J. Watson Research Lab, USA
Eijiro Sumii	Tohoku University, Japan
Walid Taha	Rice University, USA
Frank Tip	IBM T.J. Watson Research Center, USA
Philip Wadler	University of Edinburgh, UK
Joe Wells	Heriot-Watt University, UK

## External Reviewers

Umut Acar	Ashish Agarwal	Elvira Albert
Jonathan Aldrich	Tristan Oliver Richard Allwood	Puri Arenas
Aslan Askarov	Robert Atkey	Anindya Banerjee
Amir Ben-Amram	Josh Berdine	Lorenzo Bettini
Michael Beyer	Philippe Bidinger	Roderick Bloem
Eduardo Bonelli	John Boyland	Aleks Bromfield
Steve Brookes	Maria Grazia Buscemi	Diletta Romana Cacciagrano
Marco Carbone	Manuel Carro	Greg Cooper

Ricardo Corin	Andrea Corradini	Veronique Cortier
Karl Crary	Anupam Datta	Giorgio Delzanno
Mariangiola Dezani	Cinzia Di Giusto	Werner Dietl
Gabriel Ditu	Katy Dobson	Derek Dreyer
Rob Ennals	Azadeh Farzan	Boris Feigin
Maribel Fernandez	Pietro Ferrara	Robby Findler
Matthew Flatt	Florent Garnier	Samir Genaim
Prodromos Gerakios	Lars Gesellensetter	Giorgio Ghelli
Miguel Gomez-Zamalloa	Andy Gordon	Giovanna Guerrini
Thomas Göthel	Sebastian Hack	Barry Hayes
Jonathan Hayman	Paula Herber	David Herman
Kohei Honda	Haruo Hosoya	Christine Hundt
Chung-Kil Hur	Joe Hurd	Ralf Huuck
Atsushi Igarashi	Paul Jackson	Bart Jacobs
Jean-Marie Jacquet	Jan Jakubuv	Johan Jeuring
Bengt Jonsson	Gabriele Keller	Paul Kelly
Jens Knoop	Naoki Kobayashi	Giovanni Lagorio
Ivan Lanese	Alan Lawrence	Daniel Lee
Daan Leijen	Xavier Leroy	Roman Leshchinskiy
Dan Licata	Sam Lindley	Francesco Logozzo
Hans-Wolfgang Loidl	Matteo Maffei	Sergio Maffeis
Mila Majster-Cederbaum	Jonathan Mak	Keye Martin
Jacob Matthews	Conor McBride	Stephen McCamant
Jay McCarthy	Jacqueline McQuillan	Ricardo Medel
Peter Mosses	Dimitris Mostrous	Magnus O. Myreen
Gopalan Nadathur	Juan Carlos Nieves	Carlos Olarte
Paulo Oliva	Karol Ostrovsky	Scott Owens
Nikolaos Papaspyrou	Dirk Pattinson	Andrew Pitts
Arnd Poetzsch-Heffter	Didier Remy	Tamara Rezk
Tom Ridge	Stan Rosenberg	Mads Rosendahl
Alejandro Russo	Elke Salecker	Clara Segura
Peter Sewell	Robert Simmons	Christian Skalka
Gregor Snelting	Lex Spoon	Daniel Spoonhower
Sriram Srinivasan	Sam Staton	Gareth Stoyale
Tom Stuart	Henry Sudhof	Dirk Tetzlaff
Peter Thiemann	Ashish Tiwari	Viktor Vafeiadis
Frank Valencia	Pradeep Varma	Mandana Vaziri
Sven Verdoolaege	Mirko Viroli	Eelco Visser
Peng WU	Alisdair Wren	Hongwei Xi
Damiano Zanardini	Gianluigi Zavattaro	Elena Zucca



# Table of Contents

## Semantics, Parametricity, and Types

A Sound Semantics for OCaml <sub>light</sub> .....	1
<i>Scott Owens</i>	
Parametric Polymorphism through Run-Time Sealing or, Theorems for Low, Low Prices! .....	16
<i>Jacob Matthews and Amal Ahmed</i>	
Regular Expression Subtyping for XML Query and Update Languages .....	32
<i>James Cheney</i>	

## Semantics

A Theory of Hygienic Macros .....	48
<i>David Herman and Mitchell Wand</i>	
A Hybrid Denotational Semantics for Hybrid Systems .....	63
<i>Olivier Bouissou and Matthieu Martel</i>	
Full Abstraction for Linda .....	78
<i>Cinzia Di Giusto and Maurizio Gabbrielli</i>	
Practical Programming with Higher-Order Encodings and Dependent Types .....	93
<i>Adam Poswolsky and Carsten Schürmann</i>	

## Functional and Logic Programming

Programming in JoCaml (Tool Demonstration) .....	108
<i>Louis Mandel and Luc Maranget</i>	
Playing with $\mathcal{TOY}$ : Constraints and Domain Cooperation .....	112
<i>Sonia Estévez-Martín, Antonio J. Fernández, and Fernando Sáenz-Pérez</i>	
Typing Safe Deallocation .....	116
<i>Gérard Boudol</i>	
Iterative Specialisation of Horn Clauses .....	131
<i>Christoffer Rosenkilde Nielsen, Flemming Nielson, and Hanne Riis Nielson</i>	

## ESOP Invited Talk

Constructive Mathematics and Functional Programming (Abstract) . . . .	146
<i>Thierry Coquand</i>	

## Static Analysis

Ranking Abstractions . . . . .	148
<i>Aziem Chawdhary, Byron Cook, Sumit Gulwani, Mooly Sagiv, and Hongseok Yang</i>	
Non-disjunctive Numerical Domain for Array Predicate Abstraction . . . .	163
<i>Xavier Allamigeon</i>	
Upper Adjoints for Fast Inter-procedural Variable Equalities . . . . .	178
<i>Markus Müller-Olm and Helmut Seidl</i>	
Cover Algorithms and Their Combination . . . . .	193
<i>Sumit Gulwani and Madan Musuvathi</i>	

## Security I

TAPIDO: Trust and Authorization Via Provenance and Integrity in Distributed Objects (Extended Abstract) . . . . .	208
<i>Andrew Cirillo, Radha Jagadeesan, Corin Pitcher, and James Riely</i>	
Linear Declassification . . . . .	224
<i>Yûta Kaneko and Naoki Kobayashi</i>	
Just Forget It – The Semantics and Enforcement of Information Erasure . . . . .	239
<i>Sebastian Hunt and David Sands</i>	

## Concurrency

Open Bisimulation for the Concurrent Constraint Pi-Calculus . . . . .	254
<i>Maria Grazia Buscemi and Ugo Montanari</i>	
The Conversation Calculus: A Model of Service-Oriented Computation . . . . .	269
<i>Hugo T. Vieira, Luís Caires, and João C. Seco</i>	
Inferring Channel Buffer Bounds Via Linear Programming . . . . .	284
<i>Tachio Terauchi and Adam Megacz</i>	

## ETAPS Invited Talk

Verification of Higher-Order Computation: A Game-Semantic Approach . . . . .	299
<i>C.-H.L. Ong</i>	

## Program Verification

Verification of Equivalent-Results Methods .....	307
<i>K. Rustan M. Leino and Peter Müller</i>	
Semi-persistent Data Structures .....	322
<i>Sylvain Conchon and Jean-Christophe Filliâtre</i>	
A Realizability Model for Impredicative Hoare Type Theory .....	337
<i>Rasmus Lerchedahl Petersen, Lars Birkedal,</i> <i>Aleksandar Nanevski, and Greg Morrisett</i>	
Oracle Semantics for Concurrent Separation Logic .....	353
<i>Aquinas Hobor, Andrew W. Appel, and Francesco Zappa Nardelli</i>	

## Security II

Certificate Translation in Abstract Interpretation .....	368
<i>Gilles Barthe and César Kunz</i>	
A Formal Implementation of Value Commitment .....	383
<i>Cédric Fournet, Nataliya Guts, and Francesco Zappa Nardelli</i>	
Author Index .....	399