

*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*

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*

Moshe Y. Vardi

*Rice University, Houston, TX, USA*

Gerhard Weikum

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

Rocco De Nicola (Ed.)

# Programming Languages and Systems

16th European Symposium on Programming, ESOP 2007  
Held as Part of the Joint European Conferences  
on Theory and Practics of Software, ETAPS 2007  
Braga, Portugal, March 24 - April 1, 2007  
Proceedings

Volume Editor

Rocco De Nicola  
Dipartimento di Sistemi e Informatica  
Università di Firenze  
Viale Morgagni 65  
50134 Firenze, Italy  
E-mail: denicola@dsi.unifi.it

Library of Congress Control Number: 2007922404

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       3-540-71314-X Springer Berlin Heidelberg New York  
ISBN-13       978-3-540-71314-2 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 2007  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper    SPIN: 12032907    06/3142    5 4 3 2 1 0

# Foreword

ETAPS 2007 is the tenth instance of the European Joint Conferences on Theory and Practice of Software, and thus a cause for celebration.

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.

## History and Prehistory of ETAPS

ETAPS as we know it is an annual federated conference that was established in 1998 by combining five conferences [Compiler Construction (CC), European Symposium on Programming (ESOP), Fundamental Approaches to Software Engineering (FASE), Foundations of Software Science and Computation Structures (FOSSACS), Tools and Algorithms for Construction and Analysis of Systems (TACAS)] with satellite events.

All five conferences had previously existed in some form and in various collocated combinations: accordingly, the prehistory of ETAPS is complex. FOSSACS was earlier known as the Colloquium on Trees in Algebra and Programming (CAAP), being renamed for inclusion in ETAPS as its historical name no longer reflected its contents. Indeed CAAP's history goes back a long way; prior to 1981, it was known as the Colloque de Lille sur les Arbres en Algebre et en Programmation. FASE was the indirect successor of a 1985 event known as Colloquium on Software Engineering (CSE), which together with CAAP formed a joint event called TAPSOFT in odd-numbered years. Instances of TAPSOFT, all including CAAP plus at least one software engineering event, took place every two years from 1985 to 1997 inclusive. In the alternate years, CAAP took place separately from TAPSOFT.

Meanwhile, ESOP and CC were each taking place every two years from 1986. From 1988, CAAP was collocated with ESOP in even years. In 1994, CC became a "conference" rather than a "workshop" and CAAP, CC and ESOP were thereafter all collocated in even years.

TACAS, the youngest of the ETAPS conferences, was founded as an international workshop in 1995; in its first year, it was collocated with TAPSOFT. It took place each year, and became a "conference" when it formed part of ETAPS 1998. It is a telling indication of the importance of tools in the modern field of informatics that TACAS today is the largest of the ETAPS conferences.

The coming together of these five conferences was due to the vision of a small group of people who saw the potential of a combined event to be more than the sum of its parts. Under the leadership of Don Sannella, who became the first ETAPS steering committee chair, they included: Andre Arnold, Egidio Astesiano, Hartmut Ehrig, Peter Fritzsion, Marie-Claude Gaudel, Tibor Gyimothy, Paul Klint, Kim Guldstrand Larsen, Peter Mosses, Alan Mycroft, Hanne Riis Nielson, Maurice Nivat, Fernando Orejas, Bernhard Steffen, Wolfgang Thomas and (alphabetically last but in fact one of the ringleaders) Reinhard Wilhelm.

ETAPS today is a loose 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 1998–2006**

The first ETAPS took place in Lisbon in 1998. Subsequently it visited Amsterdam, Berlin, Genova, Grenoble, Warsaw, Barcelona, Edinburgh and Vienna before arriving in Braga this year. During that time it has become established as the major conference in its field, attracting participants and authors from all over the world. The number of submissions has more than doubled, and the numbers of satellite events and attendees have also increased dramatically.

### **ETAPS 2007**

ETAPS 2007 comprises five conferences (CC, ESOP, FASE, FOSSACS, TACAS), 18 satellite workshops (ACCAT, AVIS, Bytecode, COCV, FESCA, FinCo, GT-VMT, HAV, HFL, LDTA, MBT, MOMPES, OpenCert, QAPL, SC, SLA++P, TERMGRAPH and WITS), three tutorials, and seven invited lectures (not including those that were specific to the satellite events). We received around 630 submissions to the five conferences this year, giving an overall acceptance rate of 25%. To accommodate the unprecedented quantity and quality of submissions, we have four-way parallelism between the main conferences on Wednesday for the first time. Congratulations to all the authors who made it to the final programme! I hope that most of the other authors still found a way of participating in this exciting event and I hope you will continue submitting.

ETAPS 2007 was organized by the Departamento de Informática of the Universidade do Minho, 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)
- The Computer Science and Technology Center (CCTC, Universidade do Minho)
- Camara Municipal de Braga
- CeSIUM/GEMCC (Student Groups)

The organizing team comprised:

- João Saraiva (Chair)
- José Bacelar Almeida (Web site)
- José João Almeida (Publicity)
- Luís Soares Barbosa (Satellite Events, Finances)
- Victor Francisco Fonte (Web site)
- Pedro Henriques (Local Arrangements)
- José Nuno Oliveira (Industrial Liaison)
- Jorge Sousa Pinto (Publicity)
- António Nestor Ribeiro (Fundraising)
- Joost Visser (Satellite Events)

ETAPS 2007 received generous sponsorship from Fundação para a Ciência e a Tecnologia (FCT), Enabler (a Wipro Company), Cisco and TAP Air Portugal.

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

Perdita Stevens (Edinburgh, Chair), Roberto Amadio (Paris), Luciano Baresi (Milan), Sophia Drossopoulou (London), Matt Dwyer (Nebraska), Hartmut Ehrig (Berlin), José Fiadeiro (Leicester), Chris Hankin (London), Laurie Hendren (McGill), Mike Hinchey (NASA Goddard), Michael Huth (London), Anna Ingólfssdóttir (Aalborg), Paola Inverardi (L'Aquila), Joost-Pieter Katoen (Aachen), Paul Klint (Amsterdam), Jens Knoop (Vienna), Shriram Krishnamurthi (Brown), Kim Larsen (Aalborg), Tiziana Margaria (Göttingen), Ugo Montanari (Pisa), Rocco de Nicola (Florence), Jakob Rehof (Dortmund), Don Sannella (Edinburgh), João Saraiva (Minho), Vladimiro Sassone (Southampton), Helmut Seidl (Munich), Daniel Varro (Budapest), Andreas Zeller (Saarbrücken).

I would like to express my sincere gratitude to all of these people and organizations, the programme committee chairs and PC 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 2007, João Saraiva, for arranging for us to have ETAPS in the ancient city of Braga.

Edinburgh, January 2007

Perdita Stevens  
ETAPS Steering Committee Chair

# Preface

This volume contains 34 papers presented at ESOP 2007, the annual European Symposium on Programming, held in Braga, Portugal, in March 2007. The goal of ESOP has always been to bridge the gap between theory and practice of programming, and the conferences continue to be devoted to addressing fundamental issues in the specification, analysis, and implementation of programming languages and systems.

The volume begins with a summary of the invited talk by Andy Pitts and continues with the contributed ESOP papers. The papers deal with important issues such as models and languages for services, logics, type theories and other verification techniques, language-based security, static analysis and abstract interpretation, semantic theories for object-oriented languages, process algebraic techniques for proving systems properties, and term-rewriting theories.

The 34 papers contained in this volume were selected by the Program Committee out of 136 submissions, each reviewed by at least three researchers. The reviews were made by the Program Committee and by 181 additional referees, listed below. The accepted papers were selected during a two-week electronic discussion by the Program Committee.

Thanks go to the authors, the members of the Program Committee, and the external referees for their excellent work, to the ETAPS Steering Committee Chair Perdita Stevens and the ETAPS 2007 Local Organization chaired by João Saraiva for providing infrastructure and gentle reminders, and finally to Andrei Voronkov and the maintainers of the EasyChair Conference Management Systems that was very useful in all the phases of paper handling.

January 2007

Rocco De Nicola

# Organization

## Program Chair

Rocco De Nicola  
Dipartimento di Sistemi e Informatica  
Università di Firenze, Italy

## Program Committee

Steve Brookes	CMU Pittsburgh, USA
Gerard Boudol	INRIA Sophia Antipolis, France
Giuseppe Castagna	ENS Paris, France
Patrick Cousot	ENS Paris, France
Mads Dam	KTH Stockolm, Sweden
Pierpaolo Degano	Univ. Pisa, Italy
Sophia Drossopoulou	Imperial College, UK
Cedric Fournet	Microsoft Cambridge, UK
Stefania Gnesi	ISTI CNR, Italy
Joshua Guttman	MITRE, USA
Chris Hankin	Imperial College, UK
Matthew Hennessy	Univ. Sussex, UK
Alan Jeffrey	Bell Labs, USA
John Mitchell	Stanford Univ., USA
Fleming Nielson	IMM Copenhagen, Denmark
Catuscia Palamidessi	INRIA Paris, France
Benjamin Pierce	U. Pennsylvania, USA
Andrei Sabelfeld	Chalmers Univ., Sweden
Don Sannella	Univ. Edinburgh, UK
Bernhard Steffen	Univ. Dortmund, Germany
Walid Taha	Rice Univ. , USA
Jan Vitek	Purdue Univ., USA
Martin Wirsing	LMU Munich, Germany
Xavier Leroy	INRIA Paris, France
Gianluigi Zavattaro	Univ. Bologna, Italy

## Additional Referees

Andreas Abel	Tristan Allwood	Zena Ariola
Pedro Adao	Davide Ancona	Aslan Askarov
Irem Aktug	Jesus Aranda	Robert Atkey

Roberto Bagnara	Gianluigi Ferrari	Patrick Maier
Adam Barker	Gian-Luigi Ferrari	Luc Maranget
Massimo Bartoletti	Jean-Christ. Filliatre	Luca Martini
Joerg Bauer	Robby Findler	Franco Mazzanti
Hubert Baumeister	Andrea Flexeder	Hernan Melgratti
Maurice ter Beek	Nate Foster	Dale Miller
Lennart Beringer	Alain Frisch	Antoine Miné
Clara Bertolissi	Thom Frhwirth	David Monniaux
Lorenzo Bettini	Rachele Fuzzati	Anders Møller
Hariolf Betz	Fabio Gadducci	Ralf Nagel
Karthik Bhargavan	Han Gao	Sebastian Nanz
Nicole Bidoit	Stéphane Gaubert	Joachim Niehren
Gavin Bierman	Thomas Gawlitza	Christoffer R. Nielsen
Chiara Bodei	Stephen Gilmore	Peter O’Hearn
Viviana Bono	Sabine Glesner	Chris Okasaki
Marcello Bonsangue	Johan Glimming	Carlos Olarte
Michele Boreale	Jens C. Godskesen	Peter Olveckí
Gilles Brassard	Ulla Goltz	Karol Ostrovsky
Mario Bravetti	Dilian Gurov	Luca Padovani
Roberto Bruni	Rene Rydhof Hansen	Catuscia Palamidessi
Cristiano Calcagno	Fritz Henglein	Matthew Parkinson
Nick Cameron	Rolf Hennicker	Emir Pasalic
Brian Campbell	Stephan Herrmann	Marius Petria
Luca Cardelli	Mike Hicks	Andrew Phillips
Magnus Carlsson	Thomas Hildebrandt	Henrik Pilegaard
K. Chatzikokolakis	Tom Hirschowitz	Andrew Pitts
James Cheney	Matthias Hözl	Randy Pollack
Antonio Cisternino	Suresh Jagannathan	Christian W. Probst
Ricardo Corin	Johan Jeuring	Riccardo Pucella
Andrea Corradini	Stefan Kahrs	Rosario Pugliese
Antonio Cunei	Gerwin Klein	Harald Raffelt
David Cunningham	Alexander Knapp	Julian Rathke
Mika Cohen	Naoki Kobayashi	Axel Rauschmayer
Ferruccio Damiani	Ivan Lanese	Yann Regis-Gianas
Vincent Danos	Cosimo Laneve	Bernhard Reus
Olivier Danvy	Diego Latella	Tamara Rezk
Pierre-Malo Deniérou	Christopher League	M. Birna van Riemsdijk
Moshe Deutsch	Jooyong Lee	Xavier Rival
Alessandra Di Pierro	James Leifer	Alessandro Romanel
Dino Distefano	Francesca Levi	Mads Rosendahl
Kevin Donnelly	Ruy Ley-Wild	Claudio Russo
Stephan Ellner	Cedric Lhoussaine	Alejandro Russo
Moreno Falaschi	Michele Loreti	Didier Remy
Alessandro Fantechi	Markus Müller-Olm	Oliver Rütthing
Jérôme Feret	Kenneth MacKenzie	Matthew Sackman

Jens-Wolfhard Schicke  
Andreas Schroeder  
Peter Sewell  
Vitaly Shmatikov  
Jeremy Siek  
Julien Signoles  
Sam Staton  
Martin Sulzmann  
Hans Svensson  
Deian Tabakov  
Javier Thayer  
Stephan Thesing  
Alwen Tiu

Jacques Thomas  
Simon Thompson  
Alwen Tiu  
Andrew Tolmach  
Terkel K. Tolstrup  
Angelo Troina  
Frank D. Valencia  
Wim Vanhoof  
Daniele Varacca  
Betti Venneri  
Cristian Versari  
Eelco Visser  
Jan Vitek

David Walker  
Herbert Wiklicky  
Verena Wolf  
Hongwei Xi  
Zhe Yang  
Steve Zdancewic  
Noam Zeilberger  
Gefei Zhang  
Ye Zhang  
Elena Zucca  
Roberto Zunino

# Table of Contents

## Invited Talk

Techniques for Contextual Equivalence in Higher-Order, Typed Languages .....	1
<i>Andrew Pitts</i>	

## Models and Languages for Web Services

Structured Communication-Centred Programming for Web Services .....	2
<i>Marco Carbone, Kohei Honda, and Nobuko Yoshida</i>	
CC-Pi: A Constraint-Based Language for Specifying Service Level Agreements .....	18
<i>Maria Grazia Buscemi and Ugo Montanari</i>	
A Calculus for Orchestration of Web Services .....	33
<i>Alessandro Lapadula, Rosario Pugliese, and Francesco Tiezzi</i>	
A Concurrent Calculus with Atomic Transactions .....	48
<i>Lucia Acciai, Michele Boreale, and Silvano Dal Zilio</i>	

## Verification

Modal I/O Automata for Interface and Product Line Theories .....	64
<i>Kim G. Larsen, Ulrik Nyman, and Andrzej Wasowski</i>	
Using History Invariants to Verify Observers .....	80
<i>K. Rustan M. Leino and Wolfram Schulte</i>	

## Term Rewriting

On the Implementation of Construction Functions for Non-free Concrete Data Types .....	95
<i>Frédéric Blanqui, Thérèse Hardin, and Pierre Weis</i>	
Anti-pattern Matching .....	110
<i>Claude Kirchner, Radu Kopetz, and Pierre-Etienne Moreau</i>	

## Language Based Security

A Certified Lightweight Non-interference Java Bytecode Verifier .....	125
<i>Gilles Barthe, David Pichardie, and Tamara Rezk</i>	

Controlling the What and Where of Declassification in Language-Based Security ..... 141  
*Heiko Mantel and Alexander Reinhard*

Cost Analysis of Java Bytecode ..... 157  
*E. Albert, P. Arenas, S. Genaim, G. Puebla, and D. Zanardini*

**Logics and Correctness Proofs**

On the Relationship Between Concurrent Separation Logic and Assume-Guarantee Reasoning ..... 173  
*Xinyu Feng, Rodrigo Ferreira, and Zhong Shao*

Abstract Predicates and Mutable ADTs in Hoare Type Theory ..... 189  
*Aleksandar Nanevski, Amal Ahmed, Greg Morrisett, and Lars Birkedal*

Structure of a Proof-Producing Compiler for a Subset of Higher Order Logic ..... 205  
*Guodong Li, Scott Owens, and Konrad Slind*

**Static Analysis and Abstract Interpretation I**

Modular Shape Analysis for Dynamically Encapsulated Programs ..... 220  
*N. Rinetzky, A. Poetzsch-Heffter, G. Ramalingam, M. Sagiv, and E. Yahav*

Static Analysis by Policy Iteration on Relational Domains ..... 237  
*Stephane Gaubert, Eric Goubault, Ankur Taly, and Sarah Zennou*

Computing Procedure Summaries for Interprocedural Analysis ..... 253  
*Sumit Gulwani and Ashish Tiwari*

Small Witnesses for Abstract Interpretation-Based Proofs ..... 268  
*Frédéric Besson, Thomas Jensen, and Tiphaine Turpin*

**Static Analysis and Abstract Interpretation II**

Interprocedurally Analysing Linear Inequality Relations ..... 284  
*Helmut Seidl, Andrea Flexeder, and Michael Petter*

Precise Fixpoint Computation Through Strategy Iteration ..... 300  
*Thomas Gawlitza and Helmut Seidl*

**Semantic Theories for Object Oriented Languages**

A Complete Guide to the Future ..... 316  
*Frank S. de Boer, Dave Clarke, and Einar Broch Johnsen*

The Java Memory Model: Operationally, Denotationally, Axiomatically . . . . .	331
<i>Pietro Cenciarelli, Alexander Knapp, and Eleonora Sibilio</i>	
Immutable Objects for a Java-Like Language . . . . .	347
<i>C. Haack, E. Poll, J. Schäfer, and A. Schubert</i>	
<b>Process Algebraic Techniques</b>	
Scalar Outcomes Suffice for Finitary Probabilistic Testing . . . . .	363
<i>Yuxin Deng, Rob van Glabbeek, Carroll Morgan, and Chenyi Zhang</i>	
Probabilistic Anonymity Via Coalgebraic Simulations . . . . .	379
<i>Ichiro Hasuo and Yoshinobu Kawabe</i>	
A Fault Tolerance Bisimulation Proof for Consensus . . . . .	395
<i>Adrian Francalanza and Matthew Hennessy</i>	
A Core Calculus for a Comparative Analysis of Bio-inspired Calculi . . . .	411
<i>Cristian Versari</i>	
<b>Applicative Programming</b>	
A Rewriting Semantics for Type Inference . . . . .	426
<i>George Kuan, David MacQueen, and Robert Bruce Findler</i>	
Principal Type Schemes for Modular Programs . . . . .	441
<i>Derek Dreyer and Matthias Blume</i>	
A Consistent Semantics of Self-adjusting Computation . . . . .	458
<i>Umut A. Acar, Matthias Blume, and Jacob Donham</i>	
Multi-language Synchronization . . . . .	475
<i>Robert Ennals and David Gay</i>	
<b>Types for Systems Properties</b>	
Type-Based Analysis of Deadlock for a Concurrent Calculus with Interrupts . . . . .	490
<i>Kohei Suenaga and Naoki Kobayashi</i>	
Type Reconstruction for General Refinement Types . . . . .	505
<i>Kenneth Knowles and Cormac Flanagan</i>	
Dependent Types for Low-Level Programming . . . . .	520
<i>Jeremy Condit, Matthew Harren, Zachary Anderson, David Gay, and George C. Necula</i>	
<b>Author Index</b> . . . . .	537