

**Lecture Notes in Computer Science**  
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

**2028**

**Springer**

*Berlin*

*Heidelberg*

*New York*

*Barcelona*

*Hong Kong*

*London*

*Milan*

*Paris*

*Singapore*

*Tokyo*

David Sands (Ed.)

# Programming Languages and Systems

10th European Symposium on Programming, ESOP 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 Editor

David Sands  
Chalmers University of Technology and Gätebor g University  
Department of Computing Science  
412 96 Gätebor g, Sweden  
E-mail: dave@cs.chalmers.se

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Programming languages and systems : proceedings / 10th European  
Symposium on Programming, ESOP 2001, held as part of the Joint  
European Conferences on Theory and Practice of Software, ETAPS 2001,  
Genova, Italy, April 2 - 6, 2001. David Sands (ed.). - Berlin ;  
Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ;  
Singapore ; Tokyo : Springer, 2001  
(Lecture notes in computer science ; Vol. 2028)  
ISBN 3-540-41862-8

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

ISSN 0302-9743

ISBN 3-540-41862-8 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: 10782434 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, 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 Horspool (Victoria), Heinrich Hußmann (Dresden), Paul Klint (Amsterdam), Daniel Le Métayer (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

This volume contains the 28 papers presented at ESOP 2001, the Tenth European Symposium on Programming, which took place in Genova, Italy, April 4–6, 2001. The ESOP series began in 1986, and addresses both practical and theoretical issues in the design, specification, and analysis of programming languages and systems.

The call for ESOP 2001 encouraged papers addressing (but not limited to)

- Programming paradigms (including functional, logic, concurrent, and object-oriented) and their integration;
- Semantics with applications to the development of correct, secure, and efficient software and systems;
- Advanced type systems, program analysis, program transformation.

The volume begins with two invited contributions. The first contribution belongs to ETAPS as a whole, and accompanies the “unifying” ETAPS invited talk given by Luca Cardelli. The second contribution is from the ESOP invited speaker, John Mitchell. The remaining 26 papers were selected by the program committee from the 76 submissions, and include one short paper which accompanied a tool-demo presentation.

Each submission was reviewed by at least three referees, and papers were selected in the latter stages of a two week discussion phase. My thanks to the members of the program committee and other referees for their hard work. Thanks also to Christian Probst for help with the conference management software, and to Don Sannella for steering the ETAPS ship so smoothly.

January 2001

David Sands

# Organization

## Program Chair

David Sands Chalmers and Göteborg University, Sweden

## Program Committee

|                      |  |
|----------------------|--|
| Martín Abadi         | Bell Labs, USA                           |
| Radhia Cousot        | CNRS and École Polytechnique, France     |
| Mads Dam             | KTH Kista, Sweden                        |
| Andrew D. Gordon     | Microsoft Research, UK                   |
| Robert Harper        | CMU Pittsburgh, USA                      |
| Nevin Heintze        | Bell Labs, USA                           |
| Daniel Le Métayer    | Trusted Logic, France                    |
| Florence Maraninchi  | Grenoble I/Verimag, France               |
| Catuscia Palamidessi | Penn State, USA                          |
| Mooly Sagiv          | Tel-Aviv University, Israel              |
| David Sands          | Chalmers and Göteborg University, Sweden |
| Peter Sestoft        | KVL and ITU Copenhagen, Denmark          |
| Harald Søndergaard   | The University of Melbourne, Australia   |



**Additional Referees**

|                      |                   |                     |
|----------------------|-------------------|---------------------|
| Johan Agat           | Dilian Gurov      | Gordon Pace         |
| Karine Altisen       | Jörgen Gustavsson | Joachim Parrow      |
| Pierre Berlioux      | Thomas Hallgren   | Simon Peyton Jones  |
| Bruno Blanchet       | Gregoire Hamon    | Frank Pfenning      |
| Valentin Bonnard     | John Hannan       | François Pottier    |
| Glenn Bruns          | Fritz Henglein    | K. V. S. Prasad     |
| Michele Bugliesi     | Charles Hymans    | Elisa Quintarelli   |
| Luca Cardelli        | Daniel Jackson    | C.R. Ramakrishnan   |
| Giuseppe Castagna    | Thomas Jensen     | Francesco Ranzato   |
| Jan Cederquist       | Mark P. Jones     | Julian Rathke       |
| Thomas Colcombet     | Simon Jones       | Jakob Rehof         |
| Seth Copen Goldstein | Jan Jurjens       | Jon Riecke          |
| Agostino Cortesi     | Per Kreuger       | Hanne Riis Nielson  |
| Patrick Cousot       | John Lamping      | Claudio Russo       |
| Karl Crary           | Cosimo Laneve     | Andrei Sabelfeld    |
| Olivier Danvy        | Julia Lawall      | Francesca Scozzari  |
| Ewen Denney          | Peter Lee         | Ran Shaham          |
| Nachum Dershowitz    | Bjorn Lisper      | Vitaly Shmatikov    |
| Nurit Dor            | Francesco Logozzo | Zoltan Somogyi      |
| Tyson Dowd           | Renaud Marlet     | Fausto Spoto        |
| Conal Elliot         | Andres Martinelli | Peter J. Stuckey    |
| Martin Elsman        | Damien Massé      | Martin Sulzmann     |
| Jérôme Feret         | Laurent Mauborgne | Mario Südholt       |
| Cedric Fournet       | Antoine Miné      | Tommy Thorn         |
| Pascal Fradet        | David Monniaux    | Frank Valencia      |
| Nissim Francez       | Laurent Mounier   | Bjorn Victor        |
| Lars-Åke Fredlund    | Lee Naish         | Ramesh Viswanathan  |
| Stephen Freund       | Xavier Nicollin   | Jan Vitek           |
| Roberto Giacobazzi   | Thomas Noll       | Jose-Luis Vivas     |
| Pabla Giambiagi      | Martin Odersky    | David Walker        |
| Kevin Glynn          | Richard O'Keefe   | Eran Yahav          |
| Gregor Goessler      | Dino Oliva        | Amiram Yehudai      |
| Orna Grumberg        | Catherine Oriat   | Gianluigi Zavattaro |

# Table of Contents

|  |     |
|--|-----|
| A Query Language Based on the Ambient Logic .....  | 1   |
| <i>Luca Cardelli (Microsoft Research UK) and Giorgio Ghelli<br/>(Università di Pisa)</i>   |     |
| Probabilistic Polynomial-Time Process Calculus and Security Protocol<br>Analysis .....   | 23  |
| <i>John C. Mitchell (Stanford University)</i>  |     |
| A Systematic Approach to Static Access Control .....   | 30  |
| <i>François Pottier (INRIA Rocquencourt), Christian Skalka, and<br/>Scott Smith (The Johns Hopkins University)</i>   |     |
| Secure Information Flow and CPS .....  | 46  |
| <i>Steve Zdancewic and Andrew C. Myers (Cornell University)</i>  |     |
| Enforcing Safety Properties Using Type Specialization .....  | 62  |
| <i>Peter Thiemann (Universität Freiburg)</i>   |     |
| Semantics and Program Analysis of Computationally Secure Information<br>Flow .....   | 77  |
| <i>Peeter Laud (Universität des Saarlandes)</i>  |     |
| Encoding Intensional Type Analysis .....   | 92  |
| <i>Stephanie Weirich (Cornell University)</i>  |     |
| Fusion on Languages .....  | 107 |
| <i>Roland Backhouse (University of Nottingham)</i>   |     |
| Programming the Web with High-Level Programming Languages .....  | 122 |
| <i>Paul Graunke (Rice University), Shriram Krishnamurthi<br/>(Brown University), Steve Van Der Hoeven (Université de Nice),<br/>and Matthias Felleisen (Rice University)</i> |     |
| On the Completeness of Model Checking .....  | 137 |
| <i>Francesco Ranzato (Università di Padova)</i>  |     |
| Modal Transition Systems: A Foundation for Three-Valued<br>Program Analysis .....  | 155 |
| <i>Michael Huth (Kansas State University), Radha Jagadeesan (Loyola<br/>University), and David Schmidt (Kansas State University)</i>   |     |
| Entailment with Conditional Equality Constraints .....   | 170 |
| <i>Zhendong Su and Alexander Aiken (University of California, Berkeley)</i>  |     |

|  |     |
|--|-----|
| On the Complexity of Constant Propagation . . . . .  | 190 |
| <i>Markus Müller-Olm and Oliver Rüthing (Universität Dortmund)</i>   |     |
| What Are Polymorphically-Typed Ambients? . . . . .   | 206 |
| <i>Torben Amtoft, Assaf J. Kfoury, and Santiago M. Pericas-Geertsen (Boston University)</i>  |     |
| JOIN( $X$ ): Constraint-Based Type Inference for the Join-Calculus . . . . .   | 221 |
| <i>Sylvain Conchon and François Pottier (INRIA Rocquencourt)</i>   |     |
| Modular Causality in a Synchronous Stream Language . . . . .   | 237 |
| <i>Pascal Cuoq and Marc Pouzet (INRIA, Paris VI)</i>   |     |
| Control-Flow Analysis in Cubic Time . . . . .  | 252 |
| <i>Flemming Nielson (Aarhus University) and Helmut Seidl (Universität Trier)</i>   |     |
| The Recursive Record Semantics of Objects Revisited . . . . .  | 269 |
| <i>G erard Boudol (INRIA Sophia Antipolis)</i>   |     |
| A Formalisation of Java’s Exception Mechanism . . . . .  | 284 |
| <i>Bart Jacobs (University of Nijmegen)</i>  |     |
| A Formal Executable Semantics of the JavaCard Platform . . . . .   | 302 |
| <i>Gilles Barthe, Guillaume Dufay (INRIA Sophia-Antipolis),<br/>Line Jakubiec (INRIA Sophia-Antipolis and Universit e de Provence),<br/>Bernard Serpette (INRIA Sophia-Antipolis), and<br/>Sim o Melo de Sousa (INRIA Sophia-Antipolis and Universidade da<br/>Beira Interior)</i> |     |
| Modeling an Algebraic Stepper . . . . .  | 320 |
| <i>John Clements, Matthew Flatt, and Matthias Felleisen (Rice University)</i>  |     |
| Typestate Checking of Machine Code . . . . .   | 335 |
| <i>Zhichen Xu (Hewlett-Packard, Palo Alto), Thomas Reps, and<br/>Barton P. Miller (University of Wisconsin-Madison)</i>  |     |
| Proof-Directed De-compilation of Low-Level Code . . . . .  | 352 |
| <i>Shin-ya Katsumata (University of Edinburgh) and Atsushi Ohori (Japan Advanced Institute of Science and Technology)</i>  |     |
| Backwards Abstract Interpretation of Probabilistic Programs . . . . .  | 367 |
| <i>David Monniaux (LIENS, Paris)</i>   |     |
| Tool Demonstration: Finding Duplicated Code Using<br>Program Dependences . . . . .   | 383 |
| <i>Raghavan Komondoor and Susan Horwitz (University of<br/>Wisconsin-Madison)</i>  |     |

|   |            |
|---|------------|
| Compiling Problem Specifications into SAT .....   | 387        |
| <i>Marco Cadoli (Università di Roma) and Andrea Schaerf (Università di Udine)</i>   |            |
| Semantics and Termination of Simply-Moded Logic Programs with<br>Dynamic Scheduling .....   | 402        |
| <i>Annalisa Bossi (Università di Venezia), Sandro Etalle (Universiteit Maastricht and CWI Amsterdam), Sabina Rossi (Università di Venezia), and Jan-Georg Smaus (CWI Amsterdam)</i> |            |
| The Def-inite Approach to Dependency Analysis .....   | 417        |
| <i>Samir Genaim and Michael Codish (Ben-Gurion University)</i>  |            |
| <b>Author Index</b> .....   | <b>433</b> |