Lecture Notes in Computer Science 6602

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Advanced Research in Computing and Software Science
Subline of Lectures Notes in Computer Science

Gilles Barthe (Ed.)

Programming Languages and Systems

20th European Symposium on Programming, ESOP 2011
Held as Part of the Joint European Conferences
on Theory and Practice of Software, ETAPS 2011
Saarbrücken, Germany, March 26–April 3, 2011
Proceedings

Springer

Volume Editor

Gilles Barthe
IMDEA Software
Facultad de Informatica (UPM)
Campus Montegancedo, 28660 Boadilla del Monte, Madrid, Spain
E-mail: gilles.barthe@imdea.org

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-19717-8 e-ISBN 978-3-642-19718-5
DOI 10.1007/978-3-642-19718-5
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011922331

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

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

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Foreword

ETAPS 2011 was the 14th 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 the usual five sister conferences (CC, ESOP, FASE, FOSSACS, TACAS), 16 satellite workshops (ACCAT, BYTECODE, COCV, DICE, FESCA, GaLoP, GT-VMT, HAS, IWIGP, LDTA, PLACES, QAPL, ROCKS, SVARM, TERMGRAPH, and WGT), one associated event (TOSCA), and seven invited lectures (excluding those specific to the satellite events).

The five main conferences received 463 submissions this year (including 26 tool demonstration papers), 130 of which were accepted (2 tool demos), giving an overall acceptance rate of 28%. 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 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 2011 was organised by the *Universität des Saarlandes* 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)

It also had support from the following sponsors, which we gratefully thank: DFG Deutsche Forschungsgemeinschaft; AbsInt Angewandte Informatik GmbH; Microsoft Research; Robert Bosch GmbH; IDS Scheer AG / Software AG; T-Systems Enterprise Services GmbH; IBM Research; gwSaar Gesellschaft für Wirtschaftsförderung Saar mbH; Springer-Verlag GmbH; and Elsevier B.V.

The organising team comprised:

General Chair:	*Reinhard Wilhelm*
Organising Committee:	*Bernd Finkbeiner, Holger Hermanns* (chair), *Reinhard Wilhelm, Stefanie Haupert-Betz, Christa Schäfer*
Satellite Events:	*Bernd Finkbeiner*
Website:	*Hernán Baró Graf*

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

Vladimiro Sassone (Southampton, Chair), Parosh Abdulla (Uppsala), Gilles Barthe (IMDEA-Software), Lars Birkedal (Copenhagen), Michael O'Boyle (Edinburgh), Giuseppe Castagna (CNRS Paris), Marsha Chechik (Toronto), Sophia Drossopoulou (Imperial College London), Bernd Finkbeiner (Saarbrücken) Cormac Flanagan (Santa Cruz), Dimitra Giannakopoulou (CMU/NASA Ames), Andrew D. Gordon (MSR Cambridge), Rajiv Gupta (UC Riverside), Chris Hankin (Imperial College London), Holger Hermanns (Saarbrücken), Mike Hinchey (Lero, the Irish Software Engineering Research Centre), Martin Hofmann (LMU Munich), Joost-Pieter Katoen (Aachen), Paul Klint (Amsterdam), Jens Knoop (Vienna), Barbara König (Duisburg), Shriram Krishnamurthi (Brown), Juan de Lara (Madrid), Kim Larsen (Aalborg), Rustan Leino (MSR Redmond), Gerald Luettgen (Bamberg), Rupak Majumdar (Los Angeles), Tiziana Margaria (Potsdam), Ugo Montanari (Pisa), Luke Ong (Oxford), Fernando Orejas (Barcelona), Catuscia Palamidessi (INRIA Paris), George Papadopoulos (Cyprus), David Rosenblum (UCL), Don Sannella (Edinburgh), João Saraiva (Minho), Helmut Seidl (TU Munich), Tarmo Uustalu (Tallinn), and Andrea Zisman (London).

I would like to express my sincere gratitude to all of these people and organisations, the Programme Committee Chairs and members of the ETAPS conferences, the organisers of the satellite events, the speakers themselves, the many reviewers, all the participants, and Springer for agreeing to publish the ETAPS proceedings in the ARCoSS subline.

Finally, I would like to thank the Organising Chair of ETAPS 2011, Holger Hermanns and his Organising Committee, for arranging for us to have ETAPS in the most beautiful surroundings of Saarbrücken.

January 2011

Vladimiro Sassone
ETAPS SC Chair

Preface

This volume contains the papers presented at ESOP 2011, the 20th European Symposium on Programming held March 30-April 1, 2011, in Saarbrücken, Germany.

ESOP is an annual conference devoted to fundamental issues in the specification, design, analysis, and implementation of programming languages and systems. ESOP 2011 was the 20th edition in the series. The Programme Committee (PC) invited papers on all aspects of programming language research including: programming paradigms and styles, methods and tools to write and specify programs and languages, methods and tools for reasoning about programs, methods and tools for implementation, and concurrency and distribution.

Following previous editions, we maintained the page limit to 20 pages, and a rebuttal process of 72 hours during which the authors could respond to the reviews of their submission. This year, PC submissions were not allowed. We received 117 abstracts and in the end got 93 full submissions; one submission was withdrawn. The remaining 92 submissions received from 3 to 6, and on average 4, reviews; eventually the PC selected 24 papers for publication. These proceedings consist of Andrew Appel's invited paper, and of the 24 selected papers.

I would like to thank the PC and the subreviewers for their dedicated work in the paper selection process, and all authors who submitted their work to the conference. I would also like to thank the 2011 Organizing Committee, chaired by Holger Hermanns, and the Steering Committee, chaired by Vladimiro Sassone, for coordinating the organization of ETAPS 2011. Finally, I would like to thank Andrei Voronkov, whose EasyChair system proved (once more) invaluable throughout the whole process.

January 2011 Gilles Barthe

Conference Organization

Programme Chair

Gilles Barthe

Programme Committee

Nick Benton
Cristiano Calcagno
Radhia Cousot
Sophia Drossopoulou
Jean Goubault-Larrecq
Nicolas Halbwachs
Radha Jagadeesan
Gerwin Klein
Viktor Kuncak
Julia Lawall
Sorin Lerner
Frank Piessens
Arnd Poetzsch-Heffter
Francois Pottier
Shaz Qadeer
Andrey Rybalchenko
Andrei Sabelfeld
Peter Sewell
Tachio Terauchi
Vasco T. Vasconcelos
Jan Vitek
David Walker
Stephanie Weirich
Kwangkeun Yi

External Reviewers

Ahmed, Amal
Alglave, Jade
Amtoft, Torben
Ancona, Davide
Andronick, June
Askarov, Aslan
Balakrishnan, Gogul
Balland, Emilie
Banerjee, Anindya
Barnett, Michael
Berdine, Josh
Beringer, Lennart
Bertrane, Julien
Besson, Frédéric
Bierman, Gavin
Birgisson, Arnar
Bouajjani, Ahmed
Boulmé, Sylvain
Boyton, Andrew
Carbone, Marco
Casinghino, Chris
Castagna, Giuseppe
Chadha, Rohit
Chakravarty, Manuel
Chatzikokolakis, Konstantinos
Chen, Juan
Chen, Liqian
Chlipala, Adam
Choi, Wontai
Chong, Stephen
Chugh, Ravi
Cirstea, Horatiu
Comon-Lundh, Hubert
Compagnoni, Adriana
Corin, Ricardo
Cortier, Véronique
Cotton, Scott
Cremers, Cas
Crespo, Juan Manuel
D'Silva, Vijay

Daubignard, Marion
Desmet, Lieven
Devriese, Dominique
Dietl, Werner
Distefano, Dino
Dodds, Mike
Dumas, Marlon
Fahndrich, Manuel
Feller, Christoph
Feret, Jerome
Ferrara, Pietro
Filliatre, Jean-Christophe
Fournet, Cédric
Francalanza, Adrian
Gaillourdet, Jean-Marie
Gammie, Peter
Ganty, Pierre
Gay, Simon
Geilmann, Kathrin
Ghica, Dan
Gordon, Andy
Gotsman, Alexey
Goubault, Eric
Gray, Kathryn E.
Greenaway, David
Greenberg, Michael
Gupta, Ashutosh
Gurov, Dilian
Gvero, Tihomir
Hammer, Christian
Rydhof Hansen, Rene
Hedin, Daniel
Heeren, Bastiaan
Hobor, Aquinas
Honda, Kohei
Hu, Zhenjiang
Hurlin, Clément
Jacobs, Bart
Jacobs, Swen
Jaskelioff, Mauro
Jeffrey, Alan
Jensen, Simon
Jung, Yungbum
Kennedy, Andrew
Kim, Hanjun
Kim, Ik-Soon
Kim, Youil
Kinder, Johannes
Kolanski, Rafal
Kopp, Oliver
Koutavas, Vasileios
Kremer, Steve
Kunz, César
Kurnia, Ilham
König, Barbara
Laud, Peeter
Laviron, Vincent
Lee, Oukseh
Lee, Wonchan
Leroy, Xavier
Lopes, Nuno P.
Lozes, Etienne
Maffei, Matteo
Malkis, Alexander
Marinescu, Maria-Cristina
Marron, Mark
Martel, Matthieu
Martins, Francisco
Mass, Damien
Matsuda, Kazutaka
Mauborgne, Laurent
McCusker, Guy
McKinna, James
Meyer, Roland
Michaelson, Greg
Michel, Patrick
Might, Matthew
Miné, Antoine
Monniaux, David
Mostrous, Dimitris
Motika, Christian
Nguyen, Kim
Nilsson, Henrik
Noble, James
Nogueira, Pablo
Nordio, Martin
Oh, Hakjoo
Oliveira, Bruno
Owens, Scott
Pandya, Paritosh
Park, Sungwoo
Parkinson, Matthew

Petri, Gustavo
Pichardie, David
Pitcher, Corin
Plump, Detlef
Pratikakis, Polyvios
Rajan, Hridesh
Remy, Didier
Reus, Bernhard
Ringeissen, Christophe
Russo, Alejandro
Ryu, Sukyoung
Samborski-Forlese, Julian
Sands, David
Santos, André L.
Schmitt, Alan
Sevcik, Jaroslav
Shin, Jaeho
Silva, Josep
Skalka, Christian
Sozeau, Matthieu
Steffen, Martin
Strickland, Stephen T.
Summers, Alexander
Svenningsson, Josef
Thielecke, Hayo
Tsukada, Takeshi
Uustalu, Tarmo
Van Horn, David
Vanoverberghe, Dries
Venet, Arnaud
von Hanxleden, Reinhard
Wadler, Philip
Welsch, Yannick
Winwood, Simon
Yorgey, Brent
Zanella Béguelin, Santiago
Phillips, Andrew
Piskac, Ruzica
Plsek, Ales
Popeea, Corneliu
Rafnsson, Willard
Regis-Gianas, Yann
Rensink, Arend
Riba, Colin
Rompf, Tiark
Russo, Luis
S, Ramesh
Sanchez, Cesar
Sankaranarayanan, Sriram
Schaefer, Jan
Seidl, Helmut
Sewell, Thomas
Siek, Jeremy
Sjöberg, Vilhelm
Smans, Jan
Staton, Sam
Strackx, Raoul
Sumii, Eijiro
Suter, Philippe
Swierstra, Doaitse
Thiemann, Peter
Urzyczyn, Pawel
van der Meyden, Ron
van Staden, Stephan
Vaughan, Jeff
Vogels, Frederic
Vouillon, Jérôme
Wells, Joe
Westbrook, Edwin
Wrigstad, Tobias
Yu, Minlan
Zappa Nardelli, Francesco

Table of Contents

Verified Software Toolchain (Invited Talk) 1
Andrew W. Appel

Polymorphic Contracts 18
João Filipe Belo, Michael Greenberg, Atsushi Igarashi, and Benjamin C. Pierce

Proving Isolation Properties for Software Transactional Memory 38
Annette Bieniusa and Peter Thiemann

Typing Copyless Message Passing 57
Viviana Bono, Chiara Messa, and Luca Padovani

Measure Transformer Semantics for Bayesian Machine Learning 77
Johannes Borgström, Andrew D. Gordon, Michael Greenberg, James Margetson, and Jurgen Van Gael

Transfer Function Synthesis without Quantifier Elimination 97
Jörg Brauer and Andy King

Semantics of Concurrent Revisions 116
Sebastian Burckhardt and Daan Leijen

Type-Based Access Control in Data-Centric Systems 136
Luís Caires, Jorge A. Pérez, João Costa Seco, Hugo Torres Vieira, and Lúcio Ferrão

Linear Absolute Value Relation Analysis 156
Liqian Chen, Antoine Miné, Ji Wang, and Patrick Cousot

Generalizing the Template Polyhedral Domain 176
Michael A. Colón and Sriram Sankaranarayanan

Dataflow Analysis for Datarace-Free Programs 196
Arnab De, Deepak D'Souza, and Rupesh Nasre

Compiling Information-Flow Security to Minimal Trusted Computing Bases 216
Cédric Fournet and Jérémy Planul

Improving Strategies via SMT Solving 236
Thomas Martin Gawlitza and David Monniaux

Typing Local Control and State Using Flow Analysis 256
Arjun Guha, Claudiu Saftoiu, and Shriram Krishnamurthi

Barriers in Concurrent Separation Logic 276
Aquinas Hobor and Cristian Gherghina

From Exponential to Polynomial-Time Security Typing via Principal Types 297
Sebastian Hunt and David Sands

Secure the Clones: Static Enforcement of Policies for Secure Object Copying 317
Thomas Jensen, Florent Kirchner, and David Pichardie

Biochemical Reaction Rules with Constraints 338
Mathias John, Cédric Lhoussaine, Joachim Niehren, and Cristian Versari

A Testing Theory for a Higher-Order Cryptographic Language (Extended Abstract) 358
Vasileios Koutavas and Matthew Hennessy

A New Method for Dependent Parsing 378
Trevor Jim and Yitzhak Mandelbaum

Static Analysis of Run-Time Errors in Embedded Critical Parallel C Programs 398
Antoine Miné

Algorithmic Nominal Game Semantics 419
Andrzej S. Murawski and Nikos Tzevelekos

The Relationship between Separation Logic and Implicit Dynamic Frames 439
Matthew J. Parkinson and Alexander J. Summers

Precise Interprocedural Analysis in the Presence of Pointers to the Stack 459
Pascal Sotin and Bertrand Jeannet

General Bindings and Alpha-Equivalence in Nominal Isabelle 480
Christian Urban and Cezary Kaliszyk

Author Index 501