Lecture Notes in Computer Science 4963

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

Editorial Board

C.R. Ramakrishnan Jakob Rehof (Eds.)

Tools and Algorithms for the Construction and Analysis of Systems

14th International Conference, TACAS 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 Editors

C.R. Ramakrishnan
Stony Brook University
Department of Computer Science
Stony Brook, NY 11794-4400, USA
E-mail: cram@cs.sunysb.edu

Jakob Rehof
Universität Dortmund
Fachbereich Informatik
Otto-Hahn-Str. 14, 44227 Dortmund, Germany
E-mail: rehof@cs.uni-dortmund.de

Library of Congress Control Number: 2008923178

CR Subject Classification (1998): F.3, D.2.4, D.2.2, C.2.4, F.2.2

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

ISSN 0302-9743
ISBN-10 3-540-78799-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-78799-0 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12245987 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, Joaõ 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 Luettgen (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

January 2008 Vladimiro Sassone

Preface

This volume contains the proceedings of the 14th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2008) which took place in Budapest, Hungary, March 31–April 3, 2008. TACAS is a forum for researchers, developers and users interested in rigorously based tools and algorithms for the construction and analysis of systems. The conference serves to bridge the gaps between different communities that share common interests in, and techniques for, tool development and its algorithmic foundations. The research areas covered by such communities include but are not limited to formal methods, software and hardware verification, static analysis, programming languages, software engineering, real-time systems, communications protocols, and biological systems. The TACAS forum provides a venue for such communities at which common problems, heuristics, algorithms, data structures and methodologies can be discussed and explored. In doing so, TACAS aims to support researchers in their quest to improve the utility, reliability, flexibility, and efficiency of tools and algorithms for building systems.

Topics covered by the conference included, but were not limited to, the following: specification and verification techniques for finite and infinite- state systems; software and hardware verification; theorem-proving and model-checking; system construction and transformation techniques; static and run-time analysis; abstraction techniques for modeling and validation; compositional and refinement-based methodologies; testing and test-case generation; analytical techniques for secure, real-time, hybrid, safety-critical, biological or dependable systems; integration of formal methods and static analysis in high-level hardware design or software environments; tool environments and tool architectures; SAT solvers; and applications and case studies.

TACAS traditionally considers two types of papers: research papers that describe in detail novel research within the scope of the TACAS conference; and short tool demonstration papers that give an overview of a particular tool and its applications or evaluation. A total of 121 research papers and 19 tool demonstration papers were submitted to TACAS 2008 (140 submissions in total). Of these, 31 research papers and 7 tool demonstration papers were accepted. Each submission was evaluated by at least three reviewers. After a seven-week reviewing process, the program selection was carried out in a two-week electronic Program Committee meeting. We believe that the committee deliberations resulted in a strong technical program. The TACAS 2008 Program Committee selected Sharad Malik (Princeton University, USA) as invited speaker, who kindly agreed and gave a talk entitled "Hardware Verification: Techniques, Methodology and Solutions," describing specification and validation techniques for verifying emerging computing systems.

We thank the authors of submitted papers, the Program Committee members, the additional reviewers, our Tools Chair Byron Cook, and the TACAS Steering Committee. Martin Karusseit gave us prompt support for the online conference management service used to prepare this program. TACAS 2008 was part of the 11th European Joint Conference on Theory and Practice of Software (ETAPS), whose aims, organization and history are detailed in the separate foreword by the ETAPS Steering Committee Chair. We would like to express our gratitude to the ETAPS Steering Committee chaired by Vladimiro Sassone, and the Organizing Committee led by Dániel Varró for their efforts in making ETAPS 2008 a successful event.

January 2008

C. R. Ramakrishnan
Jakob Rehof

Organization

Steering Committee

Ed Brinksma	ESI and Eindhoven University of Technology, The Netherlands
Rance Cleaveland	University of Maryland, College Park & Fraunhofer USA Inc, USA
Kim Larsen	Aalborg University, Aalborg, Denmark
Bernhard Steffen	University of Dortmund, Germany
Lenore Zuck	University of Illinois, Chicago, USA

Program Committee

Patricia Bouyer	CNRS, Ecole Normale Superieure de Cachan, France
Ed Brinksma	ESI & Eindhoven University of Technology, The Netherlands
Tevfik Bultan	University of California, Santa Barbara, USA
Rance Cleaveland	University of Maryland, College Park & Fraunhofer USA Inc, USA
Byron Cook	Microsoft Research, Cambridge, UK
Bruno Dutertre	SRI, Menlo Park, USA
Patrice Godefroid	Microsoft Research, Redmond, USA
Orna Grumberg	Technion, Haifa, Israel
Aarti Gupta	NEC Laboratories America Inc, USA
Fritz Henglein	University of Copenhagen, Denmark
Michael Huth	Imperial College, London, UK
Joxan Jaffar	National University of Singapore
Kurt Jensen	University of Aarhus, Denmark
Jens Knoop	Technical University, Vienna, Austria
Barbara König	University of Duisburg-Essen, Germany
Marta Kwiatkowska	Oxford University, UK
Kim Larsen	Aalborg University, Aalborg, Denmark
Nancy Lynch	MIT, Cambridge, USA
Kedar Namjoshi	Bell Labs, Murray Hill, USA
Paul Pettersson	Mälardalen University, Sweden
Sriram Rajamani	Microsoft Research, Bangalore, India
C.R. Ramakrishnan	Stony Brook University, USA
Jakob Rehof	University of Dortmund, Germany
Bill Roscoe	Oxford University, UK
Mooly Sagiv	Tel Aviv University, Israel
Stefan Schwoon	University of Stuttgart, Germany
Bernhard Steffen	University of Dortmund, Germany
Lenore Zuck	University of Illinois, Chicago, USA

Referees

Sara Adams
Daphna Amit
Philip Armstrong
Marco Bakera
Paolo Baldan
Calin Belta
Amir Ben-Amram
Nathalie Bertrand
Per Bjesse
Bruno Blanchet
Ahmed Bouajjani
Glenn Bruns
Sven Bünte
Sebastian Burckhardt
Doron Bustan
Jan Carlson
Chunqing Chen
Ling Cheung
Wei-Ngan Chin
Alexandre David
Cristina David
Leonardo de Moura
Jyotirmoy Deshmukh
Stefan Edelkamp
AnnMarie Ericsson
Javier Esparza
Sami Evangelista
Ansgar Faenker
Harald Fecher
Elena Fersman
Andrzej Filinski
Paul Fleischer
Martin Fraenzle
Laurent Fribourg
Zhaohui Fu
Silvio Ghilardi
Robert Glück
Michael Goldsmith
Dieter Gollmann
Georges Gonthier
Alexey Gotsman
Olga Grinchtein
Marcus Groesser
Radu Grosu
Sigrid Guergens
John Håkansson
Patrik Haslum
Keijo Heljanko
Espen Højsgaard
Gerard Holzmann
Graham Hughes
Hans Hüttel
Tom Hvitved
Franjo Ivancic
Himanshu Jain
Barbara Jobstmann
Sven Joerges
Colin Johnson
Marcin Jurdzinski
Albrecht Kadlec
Vineet Kahlon
Mark Kattenbelt
Sarfraz Khurshid
Stefan Kiefer
Raimund Kirner
Felix Klaedtke
Nils Klarlund
Gerwin Klein
Pavel Krcal
Lars M. Kristensen
Daniel Kroening
Orna Kupferman
Ken Friis Larsen
Ranko Lazic
Martin Leucker
Tal Lev-Ami
Vlad Levin
Shuhao Li
Birgitta Lindström
Yang Liu
Gerald Luettgen
Kristina Lundqvist
Michael Luttenberger
Sharad Malik
Roman Manevich
Nicolas Markey
Keneth McMillan
Yael Meller
Maik Merten
Marius Mikucionis
Peter Bro Miltersen
Sayan Mitra
Torben Mogensen
Ziv Nevo
Calvin Newport
Long Nguyen
Brian Nielsen
Lasse Nielsen
Mogens Nielsen
Morten Ib Nielsen
Michael Nissen
Thomas Nolte
Tina Nolte
Aditya Nori
Gethin Norman
Ulrik Nyman
Luke Ong
Ghassan Oreiby
Rotem Oshman
Joel Ouaknine
Sam Owre
David Parker
Corina Pasareanu
Nir Piterman
Franz Puntigam
Shaz Qadeer
Harald Raffelt
Venkatesh-Prasad Ranganath
Jacob Illum Rasmussen
Clemens Renner
Pierre-Alain Reynier
Noam Rinetzky
Abhik Roychoudhury
Oliver Rüthing
Michal Rutkowski
Andrey Rybalchenko
Hassen Saidi
Arnaud Sangnier
Sriram Sankaranarayanan
Andrew Santosa

Ursula Scheben
Markus Schordan
Carsten Schürmann
Cristina Seceleanu
Sanjit Seshia
Ohad Shacham
Natarajan Shankar
A. Prasad Sistla
Harald Sondergaard
Jeremy Sproston
Jiri Srba
Jan Strejcek
Jun Sun
Daniel Sundmark
Gregoire Sutre
Dejvuth Suwimonteerabuth
Ashish Tiwari
Simon Tjell
Rachel Tzoref
Shinya Umeno
Viktor Vafeiadis
Wim van Dam
Moshe Vardi
Kapil Vaswani
Martin Vechev
Miroslav Velev
Razvan Voicu
Chao Wang
Michael Weber
Lisa M. Wells
Ingomar Wenzel
Rafael Wisniewski
Uwe Wolter
James Worrell
Michael Westergaard
Ke Xu
Avi Yadgar
Eran Yahav
Roland Yap
Greta Yorsh
Fang Yu
Michael Zolda

Table of Contents

Invited Talk

Parameterized Systems

Model Checking – I

Applications

Model Checking – II

Static Analysis

Concurrent/Distributed Systems

Tools – I

Symbolic Execution

Abstraction, Interpolation

Tools – II

Trust, Reputation