Lecture Notes in Computer Science 6015

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

Javier Esparza Rupak Majumdar (Eds.)

Tools and Algorithms for the Construction and Analysis of Systems

16th International Conference, TACAS 2010
Held as Part of the Joint European Conferences
on Theory and Practice of Software, ETAPS 2010
Paphos, Cyprus, March 20-28, 2010. Proceedings

Springer

Volume Editors

Javier Esparza
Technische Universität München
Institut für Informatik
85748 Garching, Germany
E-mail: esparza@in.tum.de

Rupak Majumdar
University of California
Department of Computer Science
Los Angeles, CA 90095, USA
E-mail: rupak@cs.ucla.edu

Library of Congress Control Number: 2010921913

CR Subject Classification (1998): F.3, D.2, C.2, D.3, D.2.4, C.3

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

ISSN 0302-9743
ISBN-10 3-642-12001-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-12001-5 Springer Berlin Heidelberg New York

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

Foreword

ETAPS 2010 was the 13th 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), 19 satellite workshops (ACCAT, ARSPA-WITS, Bytecode, CMCS, COCV, DCC, DICE, FBTC, FESCA, FOSS-AMA, GaLoP, GT-VMT, LDTA, MBT, PLACES, QAPL, SafeCert, WGT, and WRLA) and seven invited lectures (excluding those that were specific to the satellite events). The five main conferences this year received 497 submissions (including 31 tool demonstration papers), 130 of which were accepted (10 tool demos), giving an overall acceptance rate of 26%, with most of the conferences at around 24%. 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 toward 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 2010 was organised by the University of Cyprus 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 the Cyprus Tourism Organisation.

The organising team comprised:

General Chairs:	Tiziana Margaria and Anna Philippou
Local Chair:	George Papadopoulos
Secretariat:	Maria Kittira
Administration:	Petros Stratis
Satellite Events:	Anna Philippou
Website:	Konstantinos Kakousis.

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

Vladimiro Sassone (Southampton, Chair), Parosh Abdulla (Uppsala), Luca de Alfaro (Santa Cruz), Gilles Barthe (IMDEA-Software), Giuseppe Castagna (CNRS Paris), Marsha Chechik (Toronto), Sophia Drossopoulou (Imperial College London), Javier Esparza (TU Munich), 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 (LM Munich), Joost-Pieter Katoen (Aachen), Paul Klint (Amsterdam), Jens Knoop (Vienna), Shriram Krishnamurthi (Brown), Kim Larsen (Aalborg), Rustan Leino (MSR Redmond), Gerald Luettgen (Bamberg), Rupak Majumdar (Los Angeles), Tiziana Margaria (Potsdam), Ugo Montanari (Pisa), Oege de Moor (Oxford), Luke Ong (Oxford), Fernando Orejas (Barcelona) Catuscia Palamidessi (INRIA Paris), George Papadopoulos (Cyprus), David Rosenblum (UCL), Don Sannella (Edinburgh), João Saraiva (Minho), Michael Schwartzbach (Aarhus), Perdita Stevens (Edinburgh), Gabriele Taentzer (Marburg), and Martin Wirsing (LM Munich).

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 2010, George Papadopoulos, for arranging for us to have ETAPS in the most beautiful surroundings of Paphos.

January 2010 Vladimiro Sassone

Preface

This volume contains the proceedings of the 16th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2010). TACAS 2010 took place in Paphos, Cyprus, March 22–25, 2010, as part of the 13th European Joint Conferences on Theory and Practice of Software (ETAPS 2010), whose aims, organization, and history are presented in the foreword of this volume by the ETAPS Steering Committee Chair, Vladimiro Sassone.

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 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, and communications protocols. The TACAS forum provides a venue for such communities at which common problems, heuristics, algorithms, data structures, and methodologies can be discussed and explored. TACAS aims to support researchers in their quest to improve the usability, utility, flexibility, and efficiency of tools and algorithms for building systems. Tool descriptions and case studies with a conceptual message, as well as theoretical papers with clear relevance for tool construction, are all encouraged. The specific topics covered by the conference include, but are 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 safety, security, or dependability, analytical techniques for real-time, hybrid, or stochastic systems, integration of formal methods and static analysis in high-level hardware design or software environments, tool environments and tool architectures, SAT and SMT solvers, and applications and case studies.

TACAS traditionally considers two types of papers: research papers and tool demonstration papers. Research papers are full-length papers that contain novel research on topics within the scope of the TACAS conference and have a clear relevance for tool construction. Tool demonstration papers are shorter papers that give an overview of a particular tool and its applications or evaluation. TACAS 2010 received a total of 134 submissions including 24 tool demonstration papers and accepted 35 papers of which 9 papers were tool demonstration papers. Each submission was evaluated by at least three reviewers. After a six-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.

Joseph Sifakis from Verimag, France, gave the unifying ETAPS 2010 invited talk on "Embedded Systems Design — Scientific Challenges and Work Directions." The abstract of his talk is included in this volume. Jean-François Raskin from the Université Libre de Bruxelles, Belgium gave the TACAS 2010 invited talk on "Antichain Algorithms for Finite Automata."

As TACAS 2010 Program Committee Co-chairs we would like to thank the authors of all submitted papers, the Program Committee members, and all the referees for their invaluable contribution in guaranteeing such a strong technical program. We also thank the EasyChair system for hosting the conference submission and program selection process and automating much of the proceedings generation process. We would like to express our appreciation to the ETAPS Steering Committee and especially its Chair, Vladimiro Sassone, as well as the Organizing Committee for their efforts in making ETAPS 2010 such a successful event.

Finally, we remember with sadness the sudden passing of Amir Pnueli in 2009. His intellectual leadership and his patronage will be missed by the entire ETAPS community.

January 2010

Javier Esparza
Rupak Majumdar

Organization

Steering Committee

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

Program Committee

Parosh Abdulla	Uppsala University, Sweden
Josh Berdine	Microsoft Research Cambridge, UK
Armin Biere	Johannes Kepler University, Linz, Austria
Bruno Blanchet	École Normal Supérieure de Paris, France
Bernard Boigelot	University of Liège, Belgium
Rance Cleaveland	University of Maryland, College Park and Fraunhofer USA Inc., USA
Giorgio Delzanno	University of Genova, Italy
Leonardo de Moura	Microsoft Research Redmond, USA
Javier Esparza	Technische Universität München, Munich, Germany
Susanne Graf	VERIMAG, Grenoble-Gières, France
Vineet Kahlon	NEC Labs, Princeton, USA
Joost-Pieter Katoen	RWTH Aachen, Germany
Stefan Kowalewski	RWTH Aachen, Germany
Daniel Kroening	Oxford University, UK
Orna Kupferman	Hebrew University, Jerusalem, Israel
Kim G. Larsen	Aalborg University, Denmark
Rupak Majumdar	University of California, Los Angeles, USA
Ken McMillan	Cadence Berkeley Labs, USA
Madhavan Mukund	Chennai Mathematical Institute, India
Anca Muscholl	LABRI, Bordeaux, France
Doron Peled	Bar-Ilan University, Israel
C.R. Ramakrishnan	SUNY, Stony Brook, USA
S. Ramesh	GM India Science Laboratory, Bangalore, India
Sanjit Seshia	University of California, Berkeley, USA
Oleg Sokolsky	University of Pennsylvania, USA
Bernhard Steffen	University of Dortmund, Germany
Tayssir Touili	LIAFA, University of Paris 7, France
Lenore Zuck	University of Illinois, Chicago, USA

Referees

David Arney
Mohamed Faouzi Atig
Domagoj Babic
Shoham Ben-David
Jesper Bengtsson
Nikolaj Bjørner
Nicolas Blanc
Henrik Bohnenkamp
Marius Bozga
Bryan Brady
Jörg Brauer
Angelo Brillout
Robert Brummayer
Supratik Chakraborty
Satrajit Chatterjee
Taolue Chen
Yu-Fang Chen
Adam Chlipala
Hana Chockler
Rebecca Collins
Pierre Corbineau
Pepijn Crouzen
Vijay D'silva
Deepak D'Souza
Alexandre David
Manoj Dixit
Markus Doedt
Alastair Donaldson
Cezara Dragoi
Constantin Enea
Lars-Henrik Eriksson
Bernd Finkbeiner
Dana Fisman
Blaise Genest
Hugo Gimbert
Patrice Godefroid
Valentin Goranko
Dominique Gückel
Leopold Haller
Youssef Hamadi
Tingting Han
Arild M. M. Haugstad
Daniel Holcomb
Falk Howar
Radu Iosif
Himanshu Jain
David N. Jansen
Susmit Jha
Barbara Jobstmann
Kenneth Yrke Joergensen
Matti Järvisalo
Alexander Kaiser
Volker Kamin
Carsten Kern
Daniel Klink
Alexander Krauss
Jan Křetínský
Christian Kubczak
Viktor Kuncak
Anna-Lena Lamprecht
Jérôme Leroux
Shuhao Li
Wenchao Li
Rhishikesh Limaye
Kamal Lodaya
Gavin Lowe
Roman Manevich
Nicolas Markey
Matthieu Martel
Sean McLaughlin
Daniel Merschen
Roland Meyer
Marius Mikučionis
Jean-Vivien Millo
Todd Millstein
Alan Mishchenko
Swarup Mohalik
Laurent Mounier
Anders Møller
K. Narayan Kumar
Johannes Neubauer
Viet Yen Nguyen
Dejan Nickovic
Thomas Noll
David Parker
Madhusudan Parthasarathy
Mikkel Larsen Pedersen
Michael Perin
Linh Thi Xuan Phan
Andreas Podelski
Mitra Purandare
Shaz Qadeer
R. Ramanujam
Jacob Illum Rasmussen
Pascal Raymond
Ahmed Rezine
Partha Roop
Philipp Rümmer
Michal Rutkowski
Oliver Rüthing
Yaniv Sa'ar
Prahladavaradan Sampath
Sriram Sankaranarayanan
Manoranjan Satpathy
Sven Schewe
Bastian Schlich
Sylvain Schmitz
Stefan Schwoon
Cristina Seceleanu
Koushik Sen
Axel Simon
Steve Simon
Mariëlle I. A. Stoelinga
Scott Stoller
S.P. Suresh
Mark Timmer
Sinha Umeno
Frits Vaandrager
Peter van Rossum
Shobha Vasudevan
Berthold Vöcking
Tomáš Vojnar
Thomas Wahl
Igor Walukiewicz
Shaohui Wang
Andrzej Wąsowski

Nannan He
Jonathan Heinen
Keijo Heljanko
Marijn Heule
Alexander Heußner
Aditya Nori
Gethin Norman
Ulrik Nyman
Petur Olsen
Ghassan Oreiby
Carsten Weise
Georg Weissenbacher
Christoph M. Wintersteiger
Verena Wolf

Table of Contents

Invited Talks

Embedded Systems Design - Scientific Challenges and Work Directions (Abstract) 1
Joseph Sifakis

Antichain Algorithms for Finite Automata 2
Laurent Doyen and Jean-François Raskin

Probabilistic Systems and Optimization

Assume-Guarantee Verification for Probabilistic Systems 23
Marta Kwiatkowska, Gethin Norman, David Parker, and Hongyang Qu

Simple $O(m \log n)$ Time Markov Chain Lumping 38
Antti Valmari and Giuliana Franceschinis

Model Checking Interactive Markov Chains 53
Lijun Zhang and Martin R. Neuhäußer

Approximating the Pareto Front of Multi-criteria Optimization Problems 69
Julien Legriel, Colas Le Guernic, Scott Cotton, and Oded Maler

Decision Procedures

An Alternative to SAT-Based Approaches for Bit-Vectors 84
Sébastien Bardin, Philippe Herrmann, and Florian Perroud

Satisfiability Modulo the Theory of Costs: Foundations and Applications 99
Alessandro Cimatti, Anders Franzén, Alberto Griggio, Roberto Sebastiani, and Cristian Stenico

Optimal Tableau Algorithms for Coalgebraic Logics 114
Rajeev Goré, Clemens Kupke, and Dirk Pattinson

Blocked Clause Elimination 129
Matti Järvisalo, Armin Biere, and Marijn Heule

Tools I

BOOM: Taking Boolean Program Model Checking One Step Further ... 145
Gerard Basler, Matthew Hague, Daniel Kroening, C.-H. Luke Ong, Thomas Wahl, and Haoxian Zhao

The OpenSMT Solver ... 150
Roberto Bruttomesso, Edgar Pek, Natasha Sharygina, and Aliaksei Tsitovich

STRANGER: An Automata-Based String Analysis Tool for PHP ... 154
Fang Yu, Muath Alkhalaf, and Tevfik Bultan

Automata Theory

When Simulation Meets Antichains: On Checking Language Inclusion of Nondeterministic Finite (Tree) Automata ... 158
Parosh Aziz Abdulla, Yu-Fang Chen, Lukáš Holík, Richard Mayr, and Tomáš Vojnar

On Weak Modal Compatibility, Refinement, and the MIO Workbench ... 175
Sebastian S. Bauer, Philip Mayer, Andreas Schroeder, and Rolf Hennicker

Rational Synthesis ... 190
Dana Fisman, Orna Kupferman, and Yoad Lustig

Efficient Büchi Universality Checking ... 205
Seth Fogarty and Moshe Y. Vardi

Liveness

Automated Termination Analysis for Programs with Second-Order Recursion ... 221
Markus Aderhold

Ranking Function Synthesis for Bit-Vector Relations ... 236
Byron Cook, Daniel Kroening, Philipp Rümmer, and Christoph M. Wintersteiger

Fairness for Dynamic Control ... 251
Jochen Hoenicke, Ernst-Rüdiger Olderog, and Andreas Podelski

Tools II

JTorX: A Tool for On-Line Model-Driven Test Derivation and Execution ... 266
Axel Belinfante

SLAB: A Certifying Model Checker for Infinite-State Concurrent Systems 271
Klaus Dräger, Andrey Kupriyanov, Bernd Finkbeiner, and Heike Wehrheim

Tracking Heaps That Hop with Heap-Hop 275
Jules Villard, Étienne Lozes, and Cristiano Calcagno

Software Verification

Automatic Analysis of Scratch-Pad Memory Code for Heterogeneous Multicore Processors 280
Alastair F. Donaldson, Daniel Kroening, and Philipp Rümmer

Simplifying Linearizability Proofs with Reduction and Abstraction 296
Tayfun Elmas, Shaz Qadeer, Ali Sezgin, Omer Subasi, and Serdar Tasiran

A Polymorphic Intermediate Verification Language: Design and Logical Encoding 312
K. Rustan M. Leino and Philipp Rümmer

Trace-Based Symbolic Analysis for Atomicity Violations 328
Chao Wang, Rhishikesh Limaye, Malay Ganai, and Aarti Gupta

Tools III

ACS: Automatic Converter Synthesis for SoC Bus Protocols 343
Karin Avnit, Arcot Sowmya, and Jorgen Peddersen

AlPiNA: An Algebraic Petri Net Analyzer 349
Didier Buchs, Steve Hostettler, Alexis Marechal, and Matteo Risoldi

PASS: Abstraction Refinement for Infinite Probabilistic Models 353
Ernst Moritz Hahn, Holger Hermanns, Björn Wachter, and Lijun Zhang

Real Time and Information Flow

Arrival Curves for Real-Time Calculus: The Causality Problem and Its Solutions 358
Matthieu Moy and Karine Altisen

Computing the Leakage of Information-Hiding Systems 373
Miguel E. Andrés, Catuscia Palamidessi, Peter van Rossum, and Geoffrey Smith

Statistical Measurement of Information Leakage 390
Konstantinos Chatzikokolakis, Tom Chothia, and Apratim Guha

SAT Based Bounded Model Checking with Partial Order Semantics for Timed Automata 405
Janusz Malinowski and Peter Niebert

Testing

Preemption Sealing for Efficient Concurrency Testing 420
Thomas Ball, Sebastian Burckhardt, Katherine E. Coons, Madanlal Musuvathi, and Shaz Qadeer

Code Mutation in Verification and Automatic Code Correction 435
Gal Katz and Doron Peled

Efficient Detection of Errors in Java Components Using Random Environment and Restarts 451
Pavel Parizek and Tomas Kalibera

Author Index 467