

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

New York University, NY, 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

Holger Hermanns Jens Palsberg (Eds.)

Tools and Algorithms for the Construction and Analysis of Systems

12th International Conference, TACAS 2006
Held as Part of the Joint European Conferences
on Theory and Practice of Software, ETAPS 2006
Vienna, Austria, March 25 – April 2, 2006
Proceedings

Volume Editors

Holger Hermanns
Saarland University
Department of Computer Science, Dependable Systems and Software
Stuhlsatzenhausweg 45, 66123 Saarbrücken, Germany
E-mail: hermanns@cs.uni-sb.de

Jens Palsberg
University of California at Los Angeles, Computer Science Department
4531K Boelter Hall, Los Angeles, CA 90095-1596, USA
E-mail: palsberg@ucla.edu

Library of Congress Control Number: 2006922189

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 3-540-33056-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-33056-1 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

© Springer-Verlag Berlin Heidelberg 2006
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11691372 06/3142 5 4 3 2 1 0

Foreword

ETAPS 2006 was the ninth 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), 18 satellite workshops (AC-CAT, AVIS, CMCS, COCV, DCC, EAAI, FESCA, FRCSS, GT-VMT, LDTA, MBT, QAPL, SC, SLAP, SPIN, TERMGRAPH, WITS and WRLA), two tutorials, and seven invited lectures (not including those that were specific to the satellite events). We received over 550 submissions to the five conferences this year, giving an overall acceptance rate of 23%, with acceptance rates below 30% for each conference. 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.

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 loose confederation in which each event retains its own identity, with a separate Program 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 2006 was organized by the Vienna University of Technology, 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);
- Institute for Computer Languages, Vienna;
- Austrian Computing Society;
- The *Bürgermeister der Bundeshauptstadt Wien*;
- Vienna Convention Bureau;
- Intel.

The organizing team comprised:

Chair:	Jens Knoop
Local Arrangements:	Anton Ertl
Publicity:	Joost-Pieter Katoen
Satellite Events:	Andreas Krall
Industrial Liaison:	Eva Kühn
Liaison with City of Vienna:	Ulrich Neumerkel
Tutorials Chair, Website:	Franz Puntigam
Website:	Fabian Schmied
Local Organization, Workshops Proceedings:	Markus Schordan

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

Perdita Stevens (Edinburgh, Chair), Luca Aceto (Aalborg and Reykjavík), Rastislav Bodík (Berkeley), Maura Cerioli (Genova), Matt Dwyer (Nebraska), Hartmut Ehrig (Berlin), José Fiadeiro (Leicester), Marie-Claude Gaudel (Paris), Roberto Gorrieri (Bologna), Reiko Heckel (Leicester), Michael Huth (London), 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), Hanne Riis Nielson (Copenhagen), Jens Palsberg (UCLA), Mooly Sagiv (Tel-Aviv), João Saraiva (Minho), Don Sannella (Edinburgh), Vladimiro Sassone (Southampton), Helmut Seidl (Munich), Peter Sestoft (Copenhagen), Andreas Zeller (Saarbrücken).

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, the many reviewers, and Springer for agreeing to publish the ETAPS proceedings. Finally, I would like to thank the Organizing Chair of ETAPS 2006, Jens Knoop, for arranging for us to have ETAPS in the beautiful city of Vienna.

Edinburgh
January 2006

Perdita Stevens
ETAPS Steering Committee Chair

Preface

This volume contains the proceedings of the 12th TACAS, International Conference on Tools and Algorithms for the Construction and Analysis of Systems. TACAS 2006 took place in Vienna, Austria, March 27–31, 2006. TACAS is a forum for researchers, developers, and users interested in rigorously based tools for the construction and analysis of systems. The conference serves to bridge the gaps among communities that are devoted to formal methods, software and hardware verification, static analysis, programming languages, software engineering, real-time systems, and communication protocols. By providing a venue for the discussion of common problems, heuristics, algorithms, data structures, and methodologies, TACAS aims to support researchers in their quest to improve the utility, reliability, flexibility, and efficiency of tools for building systems.

Topics covered by TACAS include 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, abstract interpretation, refinement-based and compositional methodologies, testing and test-case generation, analytical techniques for security protocols, real-time, hybrid, and safety-critical systems, integration of formal methods and static analysis in high-level hardware design, tool environments and tool architectures, and applications and case studies.

TACAS traditionally considers two types of papers: full-length research papers, including those describing tools, and short tool-demonstration papers that give an overview of a particular tool and its applications. TACAS 2006 received 118 research and 9 tool-demonstration submissions, and accepted 30 research papers and 4 tool-demonstration papers. Each submission was evaluated by at least three reviewers and each submission co-authored by a PC member was evaluated by at least four reviewers. After a five-week reviewing process, the program selection was carried out in a two-week electronic Program Committee meeting. We believe that the result of the committee deliberations is a strong technical program. As this year's invited speaker, the Program Committee selected Somesh Jha, who presented work on weighted pushdown systems and trust-management systems. We thank the authors of the submitted papers, the Program Committee members, the referees, and especially the Tool Chair Thierry Jeron and the TACAS Steering Committee. Martin Karusseit gave us prompt support in dealing with the online conference management service. The help of Reza Pulungan in the general organization and the production of the proceedings is much appreciated.

TACAS 2006 was part of the 9th 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, Perdita Stevens. We would like to express our appreciation to the ETAPS Steering Committee, particularly Perdita Stevens, and the Organizing Committee for their efforts in making ETAPS 2006 a successful event.

January 2006

Holger Hermanns and Jens Palsberg
Program Committee Co-chairs

Organization

Steering Committee

Ed Brinksma	ESI and University of Twente, The Netherlands
Rance Cleaveland	SUNY, Stony Brook, USA
Kim Larsen	Aalborg University, Aalborg, Denmark
Bernhard Steffen	University of Dortmund, Dortmund, Germany
Lenore Zuck	University of Illinois, Chicago, USA

Programme Committee

Armin Biere	Johannes Kepler University, Linz, Austria
Ed Brinksma	ESI and University of Twente, The Netherlands
Gianfranco Ciardo	University of California, Riverside, USA
Alessandro Cimatti	ITC-IRST, Trento, Italy
Rance Cleaveland	SUNY, Stony Brook, USA
Hubert Garavel	INRIA Rhones-Alpes, Grenoble, France
Andy Gordon	Microsoft Research, Cambridge, UK
Orna Grumberg	Technion, Haifa, Israel
Klaus Havelund	Kestrel Technology, Palo Alto, California, USA
Holger Hermanns	Saarland University, Saarbrücken, Germany
Michael Huth	Imperial College, London, UK
Thierry Jeron	IRISA, Rennes, France
Kim Larsen	Aalborg University, Aalborg, Denmark
Ken McMillan	Cadence, Berkely, USA
Peter Niebert	University of Provence, Marseille, France
Jens Palsberg,	UCLA, Los Angeles, USA
Anna Phillipou	University of Cyprus, Nicosia, Cyprus
Jaco van de Pol	CWI, Amsterdam, The Netherlands
John Rushby	SRI, Menlo Park, USA
David Sands	Chalmers University of Technology, Goeteborg, Sweden
Helmut Seidl	Technical University of Munich, Munich, Germany
Bernhard Steffen	University of Dortmund, Dortmund, Germany
Martin Steffen	University of Kiel, Kiel, Germany
Zhendong Su	University of California, Davis, USA
Wang Yi	Uppsala University, Uppsala, Sweden
Lenore Zuck	University of Illinois, Chicago, USA

Referees

Parosh Abdulla	Andreas Grüner	Doron Peled
Erika Abraham	Dilian Gurov	Michael Petter
Wolfgang Ahrendt	Jörgen Gustavsson	Paul Pettersson
Rajeev Alur	John Håkansson	Alessandra di Pierro
Cyrille Artho	Klaus Havelund	Henrik Pilegaard
Howard Barringer	Natalia Ioustinova	HongYang Qu
Nicolas Baudru	Radha Jagadeesan	Harald Raffelt
Gerd Behrmann	David Jansen	A. Ramanujam
Saddek Bensalem	Bertrand Jeannot	Jakob Rehof
Josh Berdine	Ole Jensen	Arend Rensink
Alexandru Berlea	Lingxiao Jiang	Jan-Willem Roorde
Piergiorgio Bertoli	Sara Kalvala	Marco Roveri
Ritwik Bhattacharya	Raimund Kirner	Oliver Rüthing
Roderick Bloem	Felix Klaedtke	Theo Ruys
Stefan Blom	Peter Koppensteiner	Hassen Saidi
Patricia Bouyer	Pavel Krcal	Gwen Salaün
Marco Bozzano	Daniel Kröning	Luigi Santocanale
Laura Brandán Briones	Ruurd Kuiper	Roberto Sebastiani
Sebastien Briais	Orna Kupferman	Roberto Segala
Roberto Bruttomesso	Marcos Kurban	Simone Semprini
Jens Calamé	Marcel Kyas	Wendelin Serwe
Jan Cederquist	Rom Langerak	Sanjit Seshia
Swarat Chaudhuri	Frédéric Lang	Natarajan Shankar
Taolue Chen	Ranko Lazic	Sharon Shoham
Hana Chockler	Rustan Leino	João Marques Silva
Ming Chung	Flavio Lerda	Radu Siminiceanu
Koen Claessen	Stephen Magil	Carsten Sinz
Ricardo Corin	Roman Manevich	Doug Smith
Mohammad Dashti	Radu Mateescu	Oleg Sokolsky
Alexandre David	Teddy Matinde	Rafal Somla
Lugiez Denis	Marius Mikucionis	Jeremy Sproston
Aleksandar Dimovski	Ghassan Misherghi	Martin Steffen
Martí	Leonid Mokrushin	Mariëlle Stoelinga
n Domí	Remi Morin	Ofer Strichman
nguez	Wojciech Mostowski	Stephan Thesing
Bruno Dutertre	Markus Müller-Olm	Tayssir Touili
Cindy Eisner	Brian Nielsen	Stavros Tripakis
Harald Fecher	Ulrik Nyman	Rachel Tzoref
Jose Fiadeiro	Peter Csaba Ölveczky	Frits Vaandrager
Bernd Finkbeiner	Julien d'Orso	Helmut Veith
Emmanuel Fleury	Simona Orzan	Arnaud Venet
Anders Franzen	Karol Ostrovsky	Björn Victor
Olga Grinchtein	Corina Pasareanu	Tomas Vojnar

Uwe Waldmann
David Walker
Min Wan
Gary Wassermann

Rafael Wisniewski
Songtao Xia
Avi Yadgar
Karen Yorav

Jinqing Yu (Andy)
Hans Zantema

Table of Contents

Invited Contributions

Weighted Pushdown Systems and Trust-Management Systems <i>Somesh Jha, Stefan Schwoon, Hao Wang, Thomas Reps</i>	1
--	---

Parametrization and Slicing

Automatic Verification of Parameterized Data Structures <i>Jyotirmoy V. Deshmukh, E. Allen Emerson, Prateek Gupta</i>	27
Parameterized Verification of π -Calculus Systems <i>Ping Yang, Samik Basu, C.R. Ramakrishnan</i>	42
Easy Parameterized Verification of Biphase Mark and 8N1 Protocols <i>Geoffrey M. Brown, Lee Pike</i>	58
Evaluating the Effectiveness of Slicing for Model Reduction of Concurrent Object-Oriented Programs <i>Matthew B. Dwyer, John Hatcliff, Matthew Hoosier, Venkatesh Ranganath, Robby, Todd Wallentine</i>	73

Symbolic Techniques

New Metrics for Static Variable Ordering in Decision Diagrams <i>Radu I. Siminiceanu, Gianfranco Ciardo</i>	90
Widening ROBDDs with Prime Implicants <i>Neil Kettle, Andy King, Tadeusz Strzemecki</i>	105
Efficient Guided Symbolic Reachability Using Reachability Expressions <i>Dina Thomas, Supratik Chakraborty, Paritosh Pandya</i>	120

Satisfiability

<i>SDSAT: Tight Integration of Small Domain Encoding and Lazy Approaches in a Separation Logic Solver</i> <i>Malay K Ganai, Muralidhar Talupur, Aarti Gupta</i>	135
--	-----

SAT-Based Software Certification
Sagar Chaki 151

Expressiveness + Automation + Soundness: Towards Combining SMT Solvers and Interactive Proof Assistants
Pascal Fontaine, Jean-Yves Marion, Stephan Merz, Leonor Prensa Nieto, Alwen Tiu 167

Exploration of the Capabilities of Constraint Programming for Software Verification
Hélène Collavizza, Michel Rueher 182

Abstraction

Counterexample-Guided Abstraction Refinement for the Analysis of Graph Transformation Systems
Barbara König, Vitali Kozioura 197

Why Waste a Perfectly Good Abstraction?
Arie Gurfinkel, Marsha Chechik 212

Efficient Abstraction Refinement in Interpolation-Based Unbounded Model Checking
Bing Li, Fabio Somenzi 227

Approximating Predicate Images for Bit-Vector Logic
Daniel Kroening, Natasha Sharaygina 242

Model Checking Algorithms

Finitary Winning in ω -Regular Games
Krishnendu Chatterjee, Thomas A. Henzinger 257

Efficient Model Checking for LTL with Partial Order Snapshots
Peter Niebert, Doron Peled 272

A Local Shape Analysis Based on Separation Logic
Dino Distefano, Peter W. O’Hearn, Hongseok Yang 287

Program Verification

Compositional Model Extraction for Higher-Order Concurrent Programs
D.R. Ghica, A.S. Murawski 303

A Region Graph Based Approach to Termination Proofs <i>Stefan Leue, Wei Wei</i>	318
Verifying Concurrent Message-Passing C Programs with Recursive Calls <i>S. Chaki, E. Clarke, N. Kidd, T. Reps, T. Touili</i>	334
Automata-Based Verification of Programs with Tree Updates <i>Peter Habermehl, Radu Iosif, Tomas Vojnar</i>	350

Runtime Diagnostics

An Experimental Comparison of the Effectiveness of Control Flow Based Testing Approaches on Seeded Faults <i>Atul Gupta, Pankaj Jalote</i>	365
Exploiting Traces in Program Analysis <i>Alex Groce, Rajeev Joshi</i>	379

Quantitative Techniques

Model-Checking Markov Chains in the Presence of Uncertainties <i>Koushik Sen, Mahesh Viswanathan, Gul Agha</i>	394
Safety Metric Temporal Logic Is Fully Decidable <i>Joël Ouaknine, James Worrell</i>	411
Simulation-Based Graph Similarity <i>Oleg Sokolsky, Sampath Kannan, Insup Lee</i>	426

Tool Demonstrations

PRISM: A Tool for Automatic Verification of Probabilistic Systems <i>Andrew Hinton, Marta Kwiatkowska, Gethin Norman, David Parker</i>	441
DISTRIBUTOR and BCG_MERGE: Tools for Distributed Explicit State Space Generation <i>Hubert Garavel, Radu Mateescu, Damien Bergamini, Adrian Curic, Nicolas Descoubes, Christophe Joubert, Irina Smarandache-Sturm, Gilles Stragier</i>	445
MCMAS: A Model Checker for Multi-agent Systems <i>Alessio Lomuscio, Franco Raimondi</i>	450

MSCAN – A Tool for Analyzing MSC Specifications
Benedikt Bollig, Carsten Kern, Markus Schlütter, Volker Stolz 455

Refinement

A Practical and Complete Approach to Predicate Refinement
Ranjit Jhala, K.L. McMillan 459

Counterexample Driven Refinement for Abstract Interpretation
Bhargav S. Gulavani, Sriram K. Rajamani 474

Abstraction Refinement with Craig Interpolation and Symbolic
Pushdown Systems
Javier Esparza, Stefan Kiefer, Stefan Schwoon 489

Author Index 505