Lecture Notes in Computer Science 3440

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

Editorial Board

Nicolas Halbwachs Lenore D. Zuck (Eds.)

Tools and Algorithms for the Construction and Analysis of Systems

11th International Conference, TACAS 2005
Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2005
Edinburgh, UK, April 4-8, 2005
Proceedings

Springer

Volume Editors

Nicolas Halbwachs
Verimag/CNRS
2, avenue de Vignate, 38610 Gieres, France
E-mail: Nicolas.Halbwachs@imag.fr

Lenore D. Zuck
University of Illinois at Chicago
Department of Computer Science
851 S. Morgan Street, Chicago, Illinois 60607, USA
E-mail: lenore@cs.uic.edu

Library of Congress Control Number: 2005922497

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

ISSN 0302-9743
ISBN-10 3-540-25333-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-25333-4 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11408130 06/3142 5 4 3 2 1 0

Foreword

ETAPS 2005 was the eighth 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), 17 satellite workshops (AVIS, BYTECODE, CEES, CLASE, CMSB, COCV, FAC, FESCA, FINCO, GCW-DSE, GLPL, LDTA, QAPL, SC, SLAP, TGC, UITP), seven invited lectures (not including those that were specific to the satellite events), and several tutorials. We received over 550 submissions to the five conferences this year, giving acceptance rates below 30% for each one. Congratulations to all the authors who made it to the final program! 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 2005 was organized by the School of Informatics of the University of Edinburgh, 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).

The organizing team comprised:

- Chair: Don Sannella
- Publicity: David Aspinall
- Satellite Events: Massimo Felici

- Secretariat: Dyane Goodchild
- Local Arrangements: Monika-Jeannette Lekuse
- Tutorials: Alberto Momigliano
- Finances: Ian Stark
- Website: Jennifer Tenzer, Daniel Winterstein
- Fundraising: Phil Wadler

ETAPS 2005 received support from the University of Edinburgh.

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 Bodik (Berkeley), Maura Cerioli (Genoa), Evelyn Duesterwald (IBM, USA), Hartmut Ehrig (Berlin), José Fiadeiro (Leicester), Marie-Claude Gaudel (Paris), Roberto Gorrieri (Bologna), Reiko Heckel (Paderborn), Holger Hermanns (Saarbrücken), Joost-Pieter Katoen (Aachen), Paul Klint (Amsterdam), Jens Knoop (Vienna), Kim Larsen (Aalborg), Tiziana Margaria (Dortmund), Ugo Montanari (Pisa), Hanne Riis Nielson (Copenhagen), Fernando Orejas (Barcelona), Mooly Sagiv (Tel Aviv), Don Sannella (Edinburgh), Vladimiro Sassone (Sussex), Peter Sestoft (Copenhagen), Michel Wermelinger (Lisbon), Igor Walukiewicz (Bordeaux), Andreas Zeller (Saarbrücken), Lenore Zuck (Chicago).

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 organizer of ETAPS 2005, Don Sannella. He has been instrumental in the development of ETAPS since its beginning; it is quite beyond the limits of what might be expected that, in addition to all the work he has done as the original ETAPS Steering Committee Chairman and current ETAPS Treasurer, he has been prepared to take on the task of organizing this instance of ETAPS. It gives me particular pleasure to thank him for organizing ETAPS in this wonderful city of Edinburgh in this my first year as ETAPS Steering Committee Chair.

Edinburgh, January 2005

Perdita Stevens
ETAPS Steering Committee Chair

Preface

This volume contains the proceedings of the 11th TACAS, International Conference on *Tools and Algorithms for the Construction and Analysis of Systems*. TACAS 2005 took place in Edinburgh, UK, April 4–8, 2005. 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, compositional and refinement-based 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.

Two types of papers are traditionally considered: 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 2005 received 141 research and 20 tool demonstration submissions, and accepted 33 research papers and 8 tool demonstration papers. We'd like to thank the authors of all submitted papers.

To carry out the difficult task of selecting a program from the large number of submissions in a fair and competent manner, we were fortunate to have highly qualified Program Committee members from diverse geographic and research areas. Each submission was evaluated by at least three reviewers. After a four-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 very strong scientific program. As this year's invited speaker, the Program Committee selected Ken McMillan, who presented work on applications of Craig interpolation.

Special thanks are due to the Program Committee members and all the referees for their assistance in selecting the papers, and to Andreas Kuehlmann for his diligent work as a tool chair. The help of the TACAS Steering Committee, especially of Bernhard Steffen, was invaluable. Martin Karusseit gave us prompt support in dealing with the online conference management service.

TACAS 2005 was part of the 8th 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. In the years since it joined the ETAPS conference federation, TACAS has been the largest of the ETAPS member conferences in terms of number of submissions and papers accepted.

We would like to express our appreciation to the ETAPS Steering Committee and especially to Don Sannella and the wonderful Organizing Committee, for their efforts in making ETAPS 2005 such a successful event.

We hope to see you all in Vienna in 2006!

April 2005 Nicolas Halbwachs and Lenore Zuck

Organization

Steering Committee

Ed Brinksma	University of Twente (The Netherlands)
Rance Cleaveland	SUNY at Stony Brook (USA)
Kim Larsen	Aalborg University (Denmark)
Bernhard Steffen	University of Dortmund (Germany)

Program Committee

Rajeev Alur	University of Pennsylvania, Philadelphia (USA)
Patricia Bouyer	LSV/CNRS, Cachan (France)
Ed Brinksma	University of Twente (The Netherlands)
Randy Bryant	Carnegie Mellon University, Pittsburgh (USA)
Muffy Calder	University of Glasgow (UK)
Rance Cleaveland	University of New York at Stony Brook (USA)
Radhia Cousot	CNRS/Ecole Polytechnique, Palaiseau (France)
Cindy Eisner	IBM, Haifa (Israel)
Javier Esparza	University of Stuttgart (Germany)
Alessandro Fantechi	University of Firenze (Italy)
Patrice Godefroid	Bell Laboratories, Lisle (USA)
Andrew Gordon	Microsoft Research, Cambridge (UK)
Nicolas Halbwachs	Vérimag/CNRS, Grenoble (France)
John Hatcliff	Kansas State University (USA)
Holger Hermanns	Saarland University, Saarbruecken (Germany)
Michael Huth	Imperial College, London (UK)
Kurt Jensen	University of Aarhus, Aarhus (Denmark)
Thierry Jeron	IRISA/INRIA, Rennes (France)
Jens Knoop	Technische Universität Wien, Vienna (Austria)
Andreas Kuehlmann	Cadence Berkeley Labs, Berkeley (USA)
Marta Kwiatkowska	University of Birmingham, Birmingham (UK)
Kim Larsen	Aalborg University, Aalborg (Denmark)
Radu Mateescu	INRIA, Montbonnot (France)
Jens Palsberg	UCLA, Los Angeles (USA)
Andreas Podelski	Max-Planck-Institut für Informatik, Saarbrücken (Germany)
Sriram Rajamani	Microsoft Research, Redmond (USA)
Eli Singerman	Intel, Haifa (Israel)
Bernhard Steffen	Universität Dortmund, Dortmund (Germany)
Lenore Zuck	University of Illinois, Chicago (USA)

Referees

Erika Abraham-Mumm
Tamarah Arons
Gadiel Auerbach
Christel Baier
Ittai Balaban
Michele Banci
Clark Barrett
Gerd Behrmann
Axel Belinfante
Shoham Ben-David
Armin Biere
Henrik Bohnenkamp
Lucas Bordeaux
Laura Brandan Briones
Benoit Caillaud
Sagar Chaki
Trishul Chilimbi
Søren Christensen
Byron Cook
Pedro R. D'Argenio
Dennis Dams
Alexandre David
William Deng
Klaus Dräger
Marie Duflot
Stefan Edelkamp
Erik Ernst
Anton Ertl
Yi Fang
Sebastian Fischmeister
Dana Fisman
Cormac Flanagan
Emmanuel Fleury
Jeff Foster
Pierre Ganty
Michael Gelfond
Dan Ghica
Leonid Gluhovsky
Stefania Gnesi
Mike Gordon
Arnaud Gotlieb
Hervé Grall
Claudia Gsottberger
Peter Habermehl
Tobias Heindel
Keijo Heljanko
Jens Peter Holmegaard
Hardi Hungar
Shahid Jabbar
Lalita J. Jagadeesan
David N. Jansen
Claude Jard
Bertrand Jeannet
Ranjit Jhala
Sven Johr
Jens Bæk Jørgensen
Georg Jung
Joost-Pieter Katoen
Sagi Katz
Sharon Keidar-Barner
Barbara Koenig
Vitali Kozioura
Tomas Krilavicius
Lars M. Kristensen
Antonin Kucera
Eva Kühn
Marcos E. Kurban
Sabine Kuske
Shuvendu Lahiri
Frederic Lang
Rom Langerak
Diego Latella
Axel Legay
Jerome Leroux
Didier Lime
Yoad Lustig
Michael Luttenberger
P. Madhusudan
Thomas Mailund
Herve Marchand
Fabio Martinelli
Mieke Massink
Richard Mayr
Franco Mazzanti
Eduard Mehofer
Robert Meolic
Stephan Merz
Marius Mikucionis
David Monniaux
Laurent Mounier
Markus Mueller-Olm
Madan Musuvathi
Ralf Nagel
Mayur Naik
Elie Najm
Kedar Namjoshi
Ulrich Neumerkel
Ziv Nevo
Mogens Nielsen
Robert Nieuwenhuis
Gethin Norman
Dirk Nowotka
Robert O'Callahan
Robert Palmer
David Parker
Larry Paulson
Sophie Pinchinat
Cory Plock
Pascal Poizat
Virgile Prevosto
Reza Pulungan
Franz Puntigam
Shaz Qadeer
Ishai Rabinovitz
Harald Raffelt
Stefan Ratschan
Pascal Raymond
Jakob Rehof
Iris Reuveni
Robby
Edwin Rodriguez
Sabina Rossi
Bill Roscoe
Oliver Ruething
Vlad Rusu
Theo C. Ruys
Mooly Sagiv
Gwen Salaun
Sven Schewe
Norbert Schirmer
Markus Schordan
Stephan Schulz

Stefan Schwoon
Wendelin Serwe
Jonathan Shalev
Joseph Sifakis
Nishant Sinha
A. Prasad Sistla
Oleg Sokolsky
Emilio Spinicci
Jeremy Sproston
Jiri Srba
Mark Staples
Graham Steel
Alin Stefanescu
Marielle Stoelinga
Ofer Strichman
Andreas Tiemeyer
Cesare Tinelli
P.S. Thiagarajan
Oksana Tkachuk
Stavros Tripakis
Rachel Tzoref
Shmuel Ur
Machiel van der Bijl
Wim Vanderbauwhede
Moshe Vardi
Enrico Vicario
Farn Wang
Todd Wallentine
Andrzej Wasowski
Lisa Wells
Michael Westergaard
Wang Xu
Zijiang Yang
Wang Yi
HaiSeung Yoo
Greta Yorsh
Sergio Yovine
Håkan Younes
Lijun Zhang
Wolf Zimmermann

Table of Contents

Invited Paper

Applications of Craig Interpolants in Model Checking
Ken L. McMillan 1

Regular Model-Checking

Verifying Programs with Dynamic 1-Selector-Linked Structures in Regular Model Checking
Ahmed Bouajjani, Peter Habermehl, Pierre Moro, Tomáš Vojnar 13

Simulation-Based Iteration of Tree Transducers
Parosh Aziz Abdulla, Axel Legay, Julien d'Orso, Ahmed Rezine 30

Using Language Inference to Verify Omega-Regular Properties
Abhay Vardhan, Koushik Sen, Mahesh Viswanathan, Gul Agha 45

Infinite State Systems

On-the-Fly Reachability and Cycle Detection for Recursive State Machines
Rajeev Alur, Swarat Chaudhuri, Kousha Etessami, P. Madhusudan .. 61

Empirically Efficient Verification for a Class of Infinite-State Systems
Jesse Bingham, Alan J. Hu 77

Context-Bounded Model Checking of Concurrent Software
Shaz Qadeer, Jakob Rehof 93

A Generic Theorem Prover of CSP Refinement
Yoshinao Isobe, Markus Roggenbach 108

Abstract Interpretation

Separating Fairness and Well-Foundedness for the Analysis of Fair Discrete Systems
Amir Pnueli, Andreas Podelski, Andrey Rybalchenko 124

An Abstract Interpretation-Based Refinement Algorithm for Strong Preservation
Francesco Ranzato, Francesco Tapparo 140

Dependent Types for Program Understanding
Raghavan Komondoor, G. Ramalingam, Satish Chandra, John Field 157

Automata and Logics

A Note on On-the-Fly Verification Algorithms
Stefan Schwoon, Javier Esparza 174

Truly On-the-Fly LTL Model Checking
Moritz Hammer, Alexander Knapp, Stephan Merz 191

Complementation Constructions for Nondeterministic Automata on Infinite Words
Orna Kupferman, Moshe Y. Vardi 206

Using BDDs to Decide CTL
Will Marrero 222

Probabilistic Systems, Probabilistic Model-Checking

Model-Checking Infinite-State Markov Chains
Anne Remke, Boudewijn Haverkort, Lucia Cloth 237

Algorithmic Verification of Recursive Probabilistic State Machines
Kousha Etessami, Mihalis Yannakakis 253

Monte Carlo Model Checking
Radu Grosu, Scott A. Smolka 271

Satisfiability

Efficient Conflict Analysis for Finding All Satisfying Assignments of a Boolean Circuit
HoonSang Jin, HyoJung Han, Fabio Somenzi 287

Bounded Validity Checking of Interval Duration Logic
Babita Sharma, Paritosh K. Pandya, Supratik Chakraborty 301

An Incremental and Layered Procedure for the Satisfiability of Linear Arithmetic Logic
Marco Bozzano, Roberto Bruttomesso, Alessandro Cimatti, Tommi Junttila, Peter van Rossum, Stephan Schulz, Roberto Sebastiani 317

A Two-Tier Technique for Supporting Quantifiers in a Lazily Proof-Explicating Theorem Prover
Rustan M. Leino, Madan Musuvathi, Xinming Ou 334

Testing

Symbolic Test Selection Based on Approximate Analysis
Bertrand Jeannet, Thierry Jéron, Vlad Rusu, Elena Zinovieva 349

Symstra: A Framework for Generating Object-Oriented Unit Tests Using Symbolic Execution
Tao Xie, Darko Marinov, Wolfram Schulte, David Notkin 365

Abstraction and Reduction

Dynamic Symmetry Reduction
E. Allen Emerson, Thomas Wahl 382

Localization and Register Sharing for Predicate Abstraction
Himanshu Jain, Franjo Ivančić, Aarti Gupta, Malay K. Ganai 397

On Some Transformation Invariants Under Retiming and Resynthesis
Jie-Hong R. Jiang 413

Specification, Program Synthesis

Compositional Message Sequence Charts (CMSCs) Are Better to Implement Than MSCs
Blaise Genest 429

Temporal Logic for Scenario-Based Specifications
Hillel Kugler, David Harel, Amir Pnueli, Yuan Lu, Yves Bontemps 445

Mining Temporal Specifications for Error Detection
Westley Weimer, George C. Necula 461

A New Algorithm for Strategy Synthesis in LTL Games
Aidan Harding, Mark Ryan, Pierre-Yves Schobbens 477

Model-Checking

Shortest Counterexamples for Symbolic Model Checking of LTL with Past
Viktor Schuppan, Armin Biere 493

Snapshot Verification
Blaise Genest, Dietrich Kuske, Anca Muscholl, Doron Peled 510

Time-Efficient Model Checking with Magnetic Disk
Tonglaga Bao, Michael Jones 526

Tool Presentations

jMoped: A Java Bytecode Checker Based on Moped
Dejvuth Suwimonteerabuth, Stefan Schwoon, Javier Esparza 541

Java-MOP: A Monitoring Oriented Programming Environment for Java
Feng Chen, Grigore Roşu 546

JML-Testing-Tools: A Symbolic Animator for JML Specifications Using CLP
Fabrice Bouquet, Frédéric Dadeau, Bruno Legeard, Mark Utting 551

jETI: A Tool for Remote Tool Integration
Tiziana Margaria, Ralf Nagel, Bernhard Steffen 557

FocusCheck: A Tool for Model Checking and Debugging Sequential C Programs
Curtis W. Keller, Diptikalyan Saha, Samik Basu, Scott A. Smolka 563

SATABS: SAT-Based Predicate Abstraction for ANSI-C
Edmund Clarke, Daniel Kroening, Natasha Sharygina, Karen Yorav 570

DiVer: SAT-Based Model Checking Platform for Verifying Large Scale Systems
Malay K. Ganai, Aarti Gupta, Pranav Ashar 575

BISIMULATOR: A Modular Tool for On-the-Fly Equivalence Checking
Damien Bergamini, Nicolas Descoubes, Christophe Joubert, Radu Mateescu 581

Author Index 587