Lecture Notes in Computer Science 1384
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Bernhard Steffen (Ed.)

Tools and Algorithms for the Construction and Analysis of Systems

4th International Conference, TACAS'98
Held as Part of the Joint European Conferences
on Theory and Practice of Software, ETAPS'98
Lisbon, Portugal, March 28 – April 4, 1998
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Bernhard Steffen
Universität Dortmund, Lehrstuhl für Programmiersysteme
Fachbereich Informatik
D-44221 Dortmund, Germany
E-mail: steffen@informatik.uni-dortmund.de

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Tools and algorithms for the construction and analysis of systems : 4th international conference ; proceedings / TACAS '98, held as part of the Joint European Conferences on Theory and Practice of Software, ETAPS '98, Lisbon, Portugal, March 28 - April 4, 1998. Bernhard Steffen (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1998
(Lecture notes in computer science ; Vol. 1384)
ISBN 3-540-64356-7

CR Subject Classification (1991): F3, D.2.4, D.2.2, C.2.4

ISSN 0302-9743
ISBN 3-540-64356-7 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10632045 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Foreword

The European conference situation in the general area of software science has long been considered unsatisfactory. A fairly large number of small and medium-sized conferences and workshops take place on an irregular basis, competing for high-quality contributions and for enough attendees to make them financially viable. Discussions aiming at a consolidation have been underway since at least 1992, with concrete planning beginning in summer 1994 and culminating in a public meeting at TAPSOFT'95 in Aarhus.

On the basis of a broad consensus, it was decided to establish a single annual federated spring conference in the slot that was then occupied by TAPSOFT and CAAP/ESOP/CC, comprising a number of existing and new conferences and covering a spectrum from theory to practice. ETAPS'98, the first instance of the European Joint Conferences on Theory and Practice of Software, is taking place this year in Lisbon. It comprises five conferences (FoSSaCS, FASE, ESOP, CC, TACAS), four workshops (ACoS, VISUAL, WADT, CMCS), seven invited lectures, and nine tutorials.

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 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 natural development from its predecessors. It is a loose confederation in which each event retains its own identity, with a separate programme committee and independent 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 have hitherto been addressed in separate meetings.

ETAPS'98 has been superbly organized by José Luis Fiadeiro and his team at the Department of Informatics of the University of Lisbon. The ETAPS steering committee has put considerable energy into planning for ETAPS'98 and its successors. Its current membership is:

André Arnold (Bordeaux), Egidio Astesiano (Genova), Jan Bergstra (Amsterdam), Ed Brinksma (Enschede), Rance Cleaveland (Raleigh), Pierpaolo Degano (Pisa), Hartmut Ehrig (Berlin), José Fiadeiro (Lisbon), Jean-Pierre Finance (Nancy), Marie-Claude Gaudel (Paris), Tibor Gyimothy (Szeged), Chris Hankin (London), Stefan Jähnichen (Berlin), Uwe Kastens (Paderborn), Paul Klint (Amsterdam), Kai Koskimies (Tampere), Tom Maibaum (London), Hanne Riis Nielson (Aarhus), Fernando Orejas (Barcelona), Don Sannella (Edinburgh, chair), Bernhard Steffen (Dortmund), Doaitse Swierstra (Utrecht), Wolfgang Thomas (Kiel)

Other people were influential in the early stages of planning, including Peter Mosses (Aarhus) and Reinhard Wilhelm (Saarbrücken). ETAPS'98 has received generous sponsorship from:

Portugal Telecom
TAP Air Portugal
the Luso-American Development Foundation
the British Council
the EU programme "Training and Mobility of Researchers"
the University of Lisbon
the European Association for Theoretical Computer Science
the European Association for Programming Languages and Systems
the Gulbenkian Foundation

I would like to express my sincere gratitude to all of these people and organizations, and to José in particular, as well as to Springer-Verlag for agreeing to publish the ETAPS proceedings.

Edinburgh, January 1998

Donald Sannella
ETAPS Steering Committee chairman

Preface

This volume contains the proceedings of the 4th TACAS, International Conference on *Tools and Algorithms for the Construction and Analysis of Systems*. TACAS'98 took place at the Gulbenkian Foundation in Lisbon, Portugal, March 31st to April 3rd, 1998, as part of the First European Joint Conferences on Theory and Practice of Software (ETAPS), whose aims, organization, and history are detailed in the separate foreword by Donald Sannella.

It is the goal of TACAS to bring together researchers and practitioners interested in the development and application of tools and algorithms for specification, verification, analysis, and construction of software and hardware systems. In particular, it aims at creating an atmosphere that promotes a cross-fertilization of ideas between the different communities of theoreticians, tool builders, tool users, and system designers, in various specialized areas of computer science. In this respect, TACAS reflects the overall goal of ETAPS under a tool-oriented perspective. In fact, the scope of TACAS intersects with all the other ETAPS events, which address more traditional areas of interest.

As a consequence, in addition to the standard criteria for acceptability, contributions have also been selected on the basis of their conceptual significance in the context of neighbouring areas. This comprises the profile-driven comparison of various concepts and methods, their degree of support via interactive or fully automatic tools, and in particular case studies revealing the application profiles of the considered methods and tools.

In order to emphasize the practical importance of tools, TACAS allows tool presentations to be submitted (and reviewed) on equal footing with traditional scientific papers, treating them as 'first class citizens'. In practice, this entails their presentation in plenary conference sessions, and the integral inclusion of a tool report in the proceedings. The conference, of course, also included informal tool demonstrations, not announced in the official program.

TACAS'98 comprised

- **An invited Lecture** by Randal Bryant, the 'father' of the Binary Decisions Diagrams (BDDs), which have become over the last decade the most prominent data structures for industrially relevant tools, as well as

- **Regular Sessions** featuring 28 papers selected from 78 submissions, ranging from foundational contributions to tool presentations including online demos.

Grown itself out of a satellite meeting to TAPSOFT in 1995, TACAS'98 featured two new satellite events:

- *ACoS'98, International Workshop on Advanced Communication Services*, on April 3 – 4, and
- *VISUAL'98, International Workshop on Visualization Issues for Formal Methods*, on April 4th

selected papers of which appear in Volume 1385 of Springer Verlag's Lecture Notes in Computer Science.

TACAS'98 was hosted by the University of Lisbon, and, being part of ETAPS, it shared the excellent sponsoring and support described in Donald Sannella's foreword. Like ETAPS, TACAS will be continued next year at the University of Amsterdam, and in 2000 at the Technical University of Berlin.

Finally, warm thanks are due to the program committee and to all the referees for their assistance in selecting the papers, to Donald Sannella for mastering the coordination of the whole ETAPS, to José Luiz Fiadeiro and his local team for their brilliant organization, and, last but not least, to Claudia Herbers for her professional assistance during the last months and for her first class support in the preparation of this volume.

Dortmund, March 1998 Bernhard Steffen

Program Committee

Ed Brinksma (NL)
Rance Cleaveland (USA)
Fausto Giunchiglia (I)
Susanne Graf (F)
Tom Henzinger (USA)
Daniel Jackson (USA)
Kurt Jensen (DK)
Kim G. Larsen (DK)
Tiziana Margaria (D)
Jens Palsberg (DK)
Doron Peled (USA)
Scott Smolka (USA)
Bernhard Steffen (D, chair)
Frits Vaandrager (NL)

Referees

Rajeev Alur
Henrik Reif Andersen
Alessandro Armando
Alessandro Artale
Michael von der Beeck
M. Benerecetti
Karen Bernstein
Piergiorgio Bertoli
Ahmed Bouajjani
Marius Bozga
Francesco Calzolari
Søren Christensen
Alessandro Cimatti
Andreas Claßen
Pedro D'Argenio
Luca de Alfaro
Marco Daniele
Rob DeLine
Srinivas Devadas
Yifei Dong
Xiaoqun Du
Ansgar Fehnker
Stephen Garland
Klaus Havelund
Gerard Holzmann
Thierry Jéron
Somesh Jha
Joost Pieter Katoen
Peter Kelb
Nils Klarlund
Josva Kleist
Lars M. Kristensen
Kåre Kristoffersen
Orna Kupferman
Rom Langerak
Markus Müller-Olm
Angelika Mader
Ken McMillan
Michael Mendler
Kjeld Mortensen
Laurent Mounier
Gail Murphy
George Necula
Uwe Nestmann
Mogens Nielsen
Albert Nymeyer
Robert O'Callahan
Florence Pagani
Wojciech Penczek
Anuj Puri
Shaz Qadeer
C.R. Ramakrishnan
Pascal Raymond
Marco Roveri
Vlad Rusu
Theo Ruys
Elmer Sandvad
Roberto Sebastiani
Luciano Serafini
Arne Skou
Oleg Sokolsky
Jan Springintveld
Andrzej Szalas
Jan Tretmans
Stavros Tripakis
Antti Valmari
Moshe Vardi
Kimmo Varpaaniemi
Mandana Vazhiri
Adolfo Villafiorita
Carsten Weise
Hanno Wupper
Husnu Yenigün
Job Zwiers

Contents

Invited Lecture

Formal Verification of Pipelined Processors 1
R.E. Bryant

Regular Sessions

1. Model Checking

Fully Local and Efficient Evaluation of Alternating Fixed Points ... 5
Xinxin Liu, C.R. Ramakrishnan, S.A. Smolka

Modular Model Checking of Software 20
K. Laster, O. Grumberg

Verification Based on Local States 36
M. Huhn, P. Niebert, F. Wallner

Exploiting Symmetry in Linear Time Temporal Logic Model Checking: One Step Beyond 52
K. Ajami, S. Haddad, J.-M. Ilié

2. Design and Architecture

OPEN/CÆSAR: An Open Software Architecture for Verification, Simulation, and Testing 68
H. Garavel

Practical Model Checking Using Games 85
P. Stevens, C. Stirling

Combining Finite Automata, Parallel Programs and SDL Using Petri Nets 102
B. Grahlmann

MESA: Support for Scenario-Based Design of Concurrent Systems 118
H. Ben-Abdallah, S. Leue

3. Various Applications

Efficient Modeling of Memory Arrays in Symbolic Ternary Simulation 136
M. N. Velev, R. E. Bryant

Translation Validation 151
A. Pnueli, M. Siegel, E. Singerman

A Verified Model Checker for the Modal μ-Calculus in Coq 167
C. Sprenger

Detecting Races in Relay Ladder Logic Programs 184
A. Aiken, M. Fähndrich, Z. Su

4. Fielded Applications

Verification of Large State/Event Systems Using Compositionality and Dependency Analysis 201
J. Lind-Nielsen, H. Reif Andersen, G. Behrmann, H. Hulgaard, K. Kristoffersen, K.G. Larsen

Tamagotchis Need Not Die - Verification of STATEMATE Designs ... 217
U. Brockmeyer, G. Wittich

Modeling and Verification of sC++ Applications 232
T. Cattel

Factotum: Automatic and Systematic Sharing Support for Systems Analyzers 249
D.J. Sherman, N. Magnier

5. Verification of Real-Time Systems

Model Checking via Reachability Testing for Timed Automata 263
L. Aceto, A. Burgueño, K.G. Larsen

Formal Design and Analysis of a Gear Controller 281
M. Lindahl, P. Pettersson, W. Yi

Verifying Networks of Timed Processes 298
P. Aziz Abdulla, B. Jonsson

Model Checking of Real-Time Reachability Properties Using Abstractions 313
C. Daws, S. Tripakis

6. Mixed Analysis Techniques

Symbolic Exploration of Transition Hierarchies 330
R. Alur, T.A. Henzinger, S.K. Rajamani

Static Partial Order Reduction 345
R. Kurshan, V. Levin, M. Minea, D. Peled, H. Yenigün

Set-Based Analysis of Reactive Infinite-State Systems 358
W. Charatonik, A. Podelski

Deciding Fixed and Non-fixed Size Bit-Vectors 376
N.S. Bjørner, M.C. Pichora

7. Case Studies and Experience

Experience with Literate Programming in the Modelling and Validation of Systems 393
T.C. Ruys, E. Brinksma

A Proof of Burns N-Process Mutual Exclusion Algorithm Using Abstraction 409
H.E. Jensen, N.A. Lynch

Automated Verification of Szymanski's Algorithm 424
E.P. Gribomont, G. Zenner

Formal Verification of SDL Systems at the Siemens Mobile Phone Department 439
F. Regensburger, A. Barnard

Author Index 457