

Lecture Notes in Computer Science

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

1579

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

W. Rance Cleaveland (Ed.)

Tools and Algorithms for the Construction and Analysis of Systems

5th International Conference, TACAS'99
Held as Part of the Joint European Conferences
on Theory and Practice of Software, ETAPS'99
Amsterdam, The Netherlands, March 22-28, 1999
Proceedings



Springer

Series Editors

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

Volume Editor

W. Rance Cleaveland
State University of New York at Stony Brook
Department of Computer Science
Stony Brook, NY 11743-4400, USA
E-mail: rance@cs.sunysb.edu

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Tools and algorithms for the construction of analysis of systems : 5th international conference ; proceedings / TACAS '99, held as part of the Joint European Conferences on Theory and Practice of Software, ETAPS '99, Amsterdam, The Netherlands, March 22 - 28, 1999. W. Rance Cleaveland (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lecture notes in computer science ; Vol. 1579)
ISBN 3-540-65703-7

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

ISSN 0302-9743

ISBN 3-540-65703-7 Springer-Verlag 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-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1999
Printed in Germany

Typesetting: Camera-ready by author
SPIN 10703113 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Foreword

ETAPS'99 is the second 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 comprises five conferences (FOSSACS, FASE, ESOP, CC, TACAS), four satellite workshops (CMCS, AS, WAGA, CoFI), seven invited lectures, two invited tutorials, and six contributed 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 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. As an experiment, ETAPS'99 also includes two invited tutorials on topics of special interest. 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'99 has been organized by Jan Bergstra of CWI and the University of Amsterdam together with Frans Snijders of CWI. Overall planning for ETAPS'99 was the responsibility of the ETAPS Steering Committee, whose current membership is:

André Arnold (Bordeaux), Egidio Astesiano (Genoa), Jan Bergstra (Amsterdam), Ed Brinksma (Enschede), Rance Cleaveland (Stony Brook), Pierpaolo Degano (Pisa), Hartmut Ehrig (Berlin), José Fiadeiro (Lisbon), Jean-Pierre Finance (Nancy), Marie-Claude Gaudel (Paris), Susanne Graf (Grenoble), Stefan Jähnichen (Berlin), Paul Klint (Amsterdam), Kai Koskimies (Tampere), Tom Maibaum (London), Ugo Montanari (Pisa), Hanne Riis Nielson (Aarhus), Fernando Orejas (Barcelona), Don Sannella (Edinburgh), Gert Smolka (Saarbrücken), Doaitse Swierstra (Utrecht), Wolfgang Thomas (Aachen), Jerzy Tiuryn (Warsaw), David Watt (Glasgow)

ETAPS'98 has received generous sponsorship from:

- KPN Research
- Philips Research
- The EU programme “Training and Mobility of Researchers”
- CWI
- The University of Amsterdam
- The European Association for Programming Languages and Systems
- The European Association for Theoretical Computer Science

I would like to express my sincere gratitude to all of these people and organizations, the programme committee members of the ETAPS conferences, the organizers of the satellite events, the speakers themselves, and finally Springer-Verlag for agreeing to publish the ETAPS proceedings.

Edinburgh, January 1999

Donald Sannella
ETAPS Steering Committee Chairman

Preface

This volume contains the proceedings of the fifth international meeting on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'99). TACAS'99 took place on 22–25 March 1999 in Amsterdam as a constituent conference of the European Joint Conferences on Theory and Practice of Software (ETAPS). More information about it may be found in the foreword. Previous TACAS meetings occurred in 1998 (Lisbon), 1997 (Twente), 1996 (Passau), and 1995 (Aarhus). Like TACAS'98, TACAS'99 was a conference, while the meetings before 1998 were workshops. All previous TACAS proceedings have been published as volumes in Springer's Lecture Notes in Computer Science series.

TACAS's mission is to provide a forum for researchers, developers and users interested in rigorously based tools for the construction and analysis of systems. The conference aims to bridge the gaps between different communities — including but not limited to those devoted to formal methods, real-time, software engineering, communications protocols, hardware, theorem proving, and programming languages — that have traditionally had little interaction but share common interests in and techniques for tool development. In particular, by providing a venue for the discussion of common problems, heuristics, algorithms, data structures and methodologies, TACAS hopes to support researchers in their quest to improve the utility, reliability, flexibility and efficiency of tools for building systems.

These proceedings contain an invited paper, 28 refereed contributions, a position statement, and the text of an ETAPS tool demonstration that was reviewed independently of the TACAS program committee. The 28 regular papers were selected from 82 submissions, which represents the largest number of submissions TACAS has had to date. The accepted papers cover a wide range of topics, as the table of contents indicates, although all have relevance to the development and deployment of tools.

As Program Committee Chairman for TACAS, I would like to acknowledge the efforts of the Program Committee and paper reviewers. The obvious strength of the conference program is a testament to their thoughtful analyses of the submitted papers and to the seriousness with which they approached the selection process. I would also like to thank the other members of the TACAS Steering Committee for their guidance and advice in organizing the conference.

Stony Brook, January 1999

W. Rance Cleaveland II
Program Committee Chairman
TACAS'99

TACAS Steering Committee

Ed Brinksma (NL)
Rance Cleaveland (USA)

Kim G. Larsen (DK)
Bernhard Steffen (D)

TACAS'99 Program Committee

Chairman: Rance Cleaveland (SUNY at Stony Brook, USA)

Rajeev Alur (U. Pennsylvania, USA)	Nicolas Halbwachs (Vérimag, F)
Ed Brinksma (U. Twente, NL)	Gerard Holzmann (Bell Labs, USA)
Hubert Garavel (INRIA R.-A., F)	Kurt Jensen (U. Aarhus, DK)
Fausto Giunchiglia (U. Trento, I)	Kim G. Larsen (Aalborg U., DK)
Mike Gordon (Cambridge U., UK)	Tiziana Margaria (U. Dortmund, D)
Roberto Gorrieri (U. Bologna, I)	David Notkin (U. Washington, USA)
Jan Friso Groote (CWI, NL)	Gregor Snelting (U. Braunschweig, D)

Reviewers

Roberto Amadio	Peter K. Jensen	Doron Peled
Pedro R. D'Argenio	Burghard von Karger	Paul Pettersson
Eugene Asarin	Joost-Pieter Katoen	G. Michele Pinna
Twan Basten	Josva Kleist	Marco Pistore
Marco Bernardo	Jens Knoop	Jaco van de Pol
G�rard Berry	Dirk Kosch�tzki	L. Pomello
Roland Bol	Lars M. Kristensen	Anders P. Ravn
Volker Braun	Hee-Hwan Kwak	Michel Reniers
Mario Bravetti	Cosimo Laneve	Arend Rensink
Olaf Burkart	Rom Langerak	M. Roccetti
Paul Caspi	Izak van Langevelde	Judi Romijn
Soren Christensen	Fran cois Laroussinie	Karen Rudie
S. Cimato	Naiel Lieuwen	Vlad Rusu
Susanna Donatelli	Bas Luttik	Oliver R�thing
Kousha Etesami	Ken McMillan	Theo C. Ruys
Amy Felty	Oded Maler	Ph. Schnoebelen
Riccardo Focardi	Radu Mateescu	Mary Sheeran
Mauro Gaspari	Michael Merritt	Mihaela Sighireanu
Alain Girault	Kees Middelburg	Bernhard Steffen
Susanne Graf	Fran cois Monin	Jan Tretmans
Radu Grosu	Kjeld H. Mortensen	Stavros Tripakis
Lex Heerink	Laurent Mounier	Rene de Vries
Nevin Heintze	Markus M�ller-Olm	Jos van Wamel
Tom Henzinger	Uwe Nestmann	Carsten Weise
Holger Hermanns	Brian Nielsen	Tim Willemse
Leszek Holenderski	Oliver Niese	Sergio Yovine
Doug Howe	Thomas Noll	Gianluigi Zavattaro
Ole H. Jensen	Albert Nymeyer	Job Zwiers

Table of Contents

Invited Contribution

Modeling for Mere Mortals	1
<i>J. Kramer, J. Magee</i>	

Real-Time

Scheduling System Verification	19
<i>P.-A. Hsiung, F. Wang, Y.-S. Kuo</i>	
A Period Assignment Algorithm for Real-Time System Design	34
<i>M. Ryu, S. Hong</i>	
Analyzing Stochastic Fixed-Priority Real-Time Systems	44
<i>M. Gardner, J. Liu</i>	
Timed Diagnostics for Reachability Properties	59
<i>S. Tripakis</i>	

Case Studies

Fighting Livelock in the i-Protocol: A Comparative Study of Verification Tools	74
<i>Y. Dong, X. Du, Y. Ramakrishna, C. Ramakrishnan, I. Ramakrishnan, S. Smolka, O. Sokolsky, E. Stark, D. Warren</i>	
Proving the Soundness of a Java Bytecode Verifier Specification in Isabelle/HOL	89
<i>C. Pusch</i>	
Automated Fast-Track Reconfiguration of Group Communication Systems	104
<i>C. Kreitz</i>	
Specifications and Proofs for Ensemble Layers	119
<i>J. Hickey, N. Lynch, R. van Renesse</i>	

Compositionality and Abstraction

An Automated Analysis of Ping-Pong Interactions in E-Mail Services	134
<i>A. Bergeron, J.-C. Manzoni</i>	
Automatic Verification of Cryptographic Protocols through Compositional Analysis Techniques	148
<i>D. Marchignoli, F. Martinelli</i>	
Verification of Hierarchical State/Event Systems Using Reusability and Compositionality	163
<i>G. Behrmann, K. Larsen, H. Andersen, H. Hulgaard, J. Lind-Nielsen</i>	

On Proving Safety Properties by Integrating
 Static Analysis, Theorem Proving and Abstraction 178
V. Rusu, E. Singerman

Symbolic Analysis

Symbolic Model Checking without BDDs 193
A. Biere, A. Cimatti, E. Clarke, Y. Zhu

Symbolic Verification of Lossy Channel Systems:
 Application to the Bounded Retransmission Protocol 208
P. Abdulla, A. Annichini, A. Bouajjani

Model Checking in CLP 223
G. Delzanno, A. Podelski

Using Logic Programs with Stable Model Semantics to Solve
 Deadlock and Reachability Problems for 1-Safe Petri Nets 240
K. Heljanko

Process Algebra

Finite State Verification for the Asynchronous Pi-Calculus 255
U. Montanari, M. Pistore

Process Algebra in PVS 270
T. Basten, J. Hooman

On the Benefits of Using the Up To Techniques for
 Bisimulation Verification 285
D. Hirschhoff

Computing Strong/Weak Bisimulation Equivalences and
 Observation Congruence for Value-Passing Processes 300
Z. Li, H. Chen

Frameworks for System Construction and Analysis

Hardware Testing Using a
 Communication Protocol Conformance Testing Tool 315
H. Kahlouche, C. Vihov, M. Zendri

A Light-Weight Framework for Hardware Verification 330
C. Kern, T. Ono-Tesfaye, M. Greenstreet

An Easily Extensible Toolset for Tabular Mathematical Expressions 345
D. Peters, D.L. Parnas

From DFA-Frameworks to DFA-Generators:
 A Unifying Multiparadigm Approach 360
J. Knoop

Tool Descriptions

A Theorem Prover-Based Analysis Tool for Object-Oriented Databases ...	375
<i>D. Spelt, S. Even</i>	
DYANA: An Environment for Embedded System Design and Analysis	390
<i>A. Bakhmurov, A. Kapitonova, R. Smeliansky</i>	
Path Exploration Tool	405
<i>E. Gunter, D. Peled</i>	
Modular State Level Analysis of Distributed Systems	
Techniques and Tool Support	420
<i>P. Buchholz, P. Kemper</i>	

Position Paper

Some Issues in the Software Engineering of Verification Tools	435
<i>P. Stevens</i>	

ETAPS Tool Demonstration

The ETI Online Service in Action	439
<i>V. Braun, J. Kreidler, T. Margaria, B. Steffen</i>	

Author Index	445
---------------------------	-----