

# Lecture Notes in Computer Science

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

1785

**Springer**

*Berlin*

*Heidelberg*

*New York*

*Barcelona*

*Hong Kong*

*London*

*Milan*

*Paris*

*Singapore*

*Tokyo*

Susanne Graf   Michael Schwartzbach (Eds.)

# Tools and Algorithms for the Construction and Analysis of Systems

6th International Conference, TACAS 2000  
Held as Part of the Joint European Conferences  
on Theory and Practice of Software, ETAPS 2000  
Berlin, Germany, March 25 – April 2, 2000  
Proceedings



Springer

## Series Editors

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

## Volume Editors

Susanne Graf  
VERIMAG  
2, Avenue de la Vignate, 38240 Gières, France  
E-mail: Susanne.Graf@imag.fr

Michael Schwartzbach  
University of Aarhus  
BRICS, Department of Computer Science  
Ny Munkegade, 8000 Aarhus C, Denmark  
E-mail: mis@daimi.aau.dk

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Tools and algorithms for the construction and analysis of systems :  
6th international conference ; proceedings / TACAS 2000, held as part  
of the Joint European Conferences on Theory and Practice of Software,  
ETAPS 2000, Berlin, Germany, March 25 - April 2, 2000. Susanne Graf ;  
Michael Schwartzbach (ed.). - Berlin ; Heidelberg ; New York ;  
Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo :  
Springer, 2000  
(Lecture notes in computer science ; Vol. 1785)  
ISBN 3-540-67282-6

CR Subject Classification (1991): F.3, D.2.4, D.2.2, C.2.4, F.2.2

ISSN 0302-9743

ISBN 3-540-67282-6 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 is a company in the BertelsmannSpringer publishing group.  
© Springer-Verlag Berlin Heidelberg 2000  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by DA-Tex Gerd Blumenstein  
Printed on acid-free paper      SPIN 10719978      06/3142      5 4 3 2 1 0

# Foreword

ETAPS 2000 was the third 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 (FOSSACS, FASE, ESOP, CC, TACAS), five satellite workshops (CBS, CMCS, CoFI, GRATRA, INT), seven invited lectures, a panel discussion, and ten 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 program 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 were formerly addressed in separate meetings. The program of ETAPS 2000 included a public business meeting where participants had the opportunity to learn about the present and future organization of ETAPS and to express their opinions about what is bad, what is good, and what might be improved.

ETAPS 2000 was hosted by the Technical University of Berlin and was efficiently organized by the following team:

Bernd Mahr (General Chair)  
Hartmut Ehrig (Program Coordination)  
Peter Pepper (Organization)  
Stefan Jähnichen (Finances)  
Radu Popescu-Zeletin (Industrial Relations)

with the assistance of BWO Marketing Service GmbH. The publicity was superbly handled by Doris Fährndrich of the TU Berlin with assistance from the ETAPS publicity chair, Andreas Podelski. Overall planning for ETAPS conferences is the responsibility of the ETAPS steering committee, whose current membership is:

Egidio Astesiano (Genova), Jan Bergstra (Amsterdam), Pierpaolo Degano (Pisa), Hartmut Ehrig (Berlin), José Fiadeiro (Lisbon), Marie-Claude Gaudel (Paris), Susanne Graf (Grenoble), Furio Honsell (Udine), Heinrich Hußmann (Dresden), Stefan Jähnichen (Berlin), Paul Klint (Amsterdam), Tom Maibaum (London), Tiziana Margaria (Dortmund), Ugo Montanari (Pisa), Hanne Riis Nielson (Aarhus), Fernando Orejas (Barcelona), Andreas Podelski (Saarbrücken), David Sands (Göteborg), Don Sannella (Edinburgh), Gert Smolka (Saarbrücken), Bernhard Steffen (Dortmund), Wolfgang Thomas (Aachen), Jerzy Tiuryn (Warsaw), David Watt (Glasgow), Reinhard Wilhelm (Saarbrücken)

ETAPS 2000 received generous sponsorship from:

the Institute for Communication and Software Technology of TU Berlin  
the European Association for Programming Languages and Systems  
the European Association for Theoretical Computer Science  
the European Association for Software Development Science  
the “High-Level Scientific Conferences” component of the European  
Commission’s Fifth Framework Programme

I would like to express my sincere gratitude to all of these people and organizations, the program 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.

January 2000

Donald Sannella  
ETAPS Steering Committee Chairman

# Preface

This volume contains the proceedings of the 6th TACAS, International Conference on **T**ools and **A**lgorithms for the **C**onstruction and **A**nalysis of **S**ystems. TACAS took place at the Technical University of Berlin, March 27–31, 2000, as a part of the third European Joint Conferences on Theory and Practice of Software (ETAPS) whose aims and organization are detailed in a separate foreword by Don Sannella.

Previous TACAS meetings were held in 1999 (Amsterdam), 1998 (Lisbon), 1997 (Twente), 1996 (Passau), and 1995 (Aarhus). Since 1998 TACAS has been a conference and part of ETAPS. All previous TACAS proceedings have been published as volumes in Springer-Verlag's Lecture Notes in Computer Science series.

It is the goal of TACAS to provide a forum for researchers, developers, and users interested in the development and application of tools for the specification, verification, analysis, and construction of software and hardware systems. In particular, it aims to promote the exchange of ideas between different communities of theoreticians, tool builders, tool users, and system designers of various specialized areas that traditionally had little interaction. In this respect, TACAS reflects the overall goal of ETAPS from a tool oriented perspective. In effect, the scope of TACAS intersects with those of all 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 neighbouring areas. This comprises the comparison of concepts and methods, their degree of support via interactive or fully automatic tools, and case studies revealing the application profiles of the considered methods and tools.

In order to emphasize the practical importance of tools, TACAS encourages tool presentations on equal footing with traditional scientific papers, treating them as “first class citizens”. In practice, this means that they have the same space in the proceedings and a full slot in the plenary conference session. Of course, during the conference there were also demonstrations of tools not announced in the official program.

These proceedings contain

- **an invited lecture** by Pierre Wolper and Bernhard Boigelot from the University of Liège “*On the Construction of Automata from Linear Arithmetic Constraints*”.
- **33 regular contributions**, covering a wide range of topics and being all relevant to the development of tools. They have been selected from 107 submissions, which is the largest number of submission TACAS has had so far.
- the text of two **short tool demonstrations** which were reviewed by the ETAPS steering committee.

TACAS was hosted by the Technical University of Berlin, and being part of ETAPS, it shared the excellent organization described by Don Sannella in the foreword. TACAS will be continued next year as a part of ETAPS at Genova and in 2002 in Grenoble.

Finally, we would like to thank the program committee and all the referees for their assistance in selecting the papers, Don Sannella for mastering the coordination of the whole ETAPS, and last but not least, the local organizers in Berlin.

January 2000

Susanne Graf  
Michael Schwartzbach

## Steering Committee

Ed Brinksma (U. Twente)  
Rance Cleaveland (SUNY at Stony Brook)  
Kim G. Larsen (U. Aalborg)  
Bernhard Steffen (U. Dortmund)

## Program Committee

**Chairs:** Susanne Graf (VERIMAG, Grenoble)  
Michael Schwartzbach (BRICS, Aarhus)

Thomas Ball (Microsoft Research)	Joost Kok (U. Leiden)
Ed Brinksma (U. Twente)	Kim Larsen (U. Aalborg)
Rance Cleaveland (Stony Brook)	Tiziana Margaria (U. Dortmund)
Matthew Dwyer (Kansas State U.)	Bernhard Steffen (U. Dortmund)
Fausto Giunchiglia (U. Trento)	Perdita Stevens (U. Edinburgh)
Constance Heitmeyer (Naval Research)	Wang Yi (U. Uppsala)
Gerard Holzmann (Bell Labs)	
Claude Jard (IRISA, Rennes)	



## Reviewers

Parosh Abdulla	Holger Hermanns	Markus Müller-Olm
Rajeev Alur	Andreas Holzmann	Gustaf Naeser
Tobias Amnell	Juraj Hromkovic	Kedar Namjoshi
Stuart Anderson	Frank Huch	Uwe Nestmann
Myla M. Archer	Thomas Hune	Peter Niebert
Mark Ardis	Hardi Hungar	Oliver Niese
Eugène Asarin	Purush Iyer	Marcus Nilsson
David Aspinall	Paul Jackson	Thomas Noll
Gerd Behrmann	Ralph Jeffords	Jan Nyström
Johan Bengtsson	Henrik E. Jensen	Corina Pasareanu
Saddek Bensalem	Peter K. Jensen	Doron Peled
Ramesh Bharadwaj	Thierry Jeron	Paul Pettersson
Roland Bol	Mark Jerrum	Xu Qiwen
Marcello Bonsangue	Bengt Jonsson	Sriram Rajamani
Ahmed Bouajjani	Pim Kars	Arend Rensink
Julian Bradfield	Joost-Pieter Katoen	Marina Ribaud
Volker Braun	Tim Kempster	Søren Riis
Paul Caspi	Yonit Kesten	Judi Romijn
Frederico Crazzolaro	James Kirby	Mauno Ronkko
Pedro D'Argenio	Nils Klarlund	Vlad Rusu
Mads Dam	Jens Knoop	Oliver Rüthing
Achim Dannecker	Kaare J. Kristoffersen	Theo Ruys
Alexandre David	Yassine Lakhnech	Konstantinos Sagonas
Rick Dewar	Rom Langerak	Wolfram Schulte
Rolf Drechsler	Elizabeth Leonard	Joseph Sifakis
Jakob Engblom	Martin Leucker	Mikael Sjodin
Harald Ganzinger	Jorn Lind-Nielsen	Arne Skou
Stephen Gilmore	Hans Henrik Løvengreen	Margaret H. Smith
Jens Chr. Godskesen	Angelika Mader	Colin Stirling
David Griffioen	Thomas Mailund	Jan Tretmans
Corin Gurr	Oded Maler	Stavros Tripakis
Michael Hanus	Radu Mateescu	Judith Underwood
John Hatcliff	Michael Mendler	Glynn Winskel
Klaus Havelund	Faron Moller	Sergio Yovine
Loïc Hélouët	Laurent Mounier	René de Vries
Jesper G. Henriksen	Anders Møller	

# Table of Contents

## Invited Contribution

On the Construction of Automata from Linear Arithmetic Constraints .....	1
<i>Pierre Wolper and Bernard Boigelot</i>	

## Software and Formal Methods Tools

An Extensible Type System for Component-Based Design .....	20
<i>Yuhong Xiong and Edward A. Lee</i>	
Proof General: A Generic Tool for Proof Development .....	38
<i>David Aspinall</i>	
ViewPoint-Oriented Software Development: Tool Support for Integrating Multiple Perspectives by Distributed Graph Transformation .....	43
<i>Michael Goedicke, Bettina Enders, Torsten Meyer and Gabriele Taentzer</i>	

## Formal Methods Tools

Consistent Integration of Formal Methods .....	48
<i>Peter Braun, Heiko Lötzbeyer, Bernhard Schätz and Oscar Slotosch</i>	
An Architecture for Interactive Program Provers .....	63
<i>Jörg Meyer and Arnd Poetzsch-Heffter</i>	
The PROSPER Toolkit .....	78
<i>Louise A. Dennis, Graham Collins, Michael Norrish, Richard Boulton, Konrad Slind, Graham Robinson, Mike Gordon and Tom Melham</i>	
CASL: From Semantics to Tools .....	93
<i>Till Mossakowski</i>	

## Timed and Hybrid Systems

On the Construction of Live Timed Systems .....	109
<i>Sébastien Bornot, Gregor Gößler and Joseph Sifakis</i>	
On Memory-Block Traversal Problems in Model-Checking Timed Systems .....	127
<i>Fredrik Larsson, Paul Pettersson and Wang Yi</i>	
Symbolic Model Checking for Rectangular Hybrid Systems .....	142
<i>Thomas A. Henzinger and Rupak Majumdar</i>	

Efficient Data Structure for Fully Symbolic Verification of Real-Time Software Systems .....	157
<i>Farn Wang</i>	

## Infinite and Parameterized Systems

Verification of Parameterized Systems Using Logic Program Transformations .....	172
<i>Abhik Roychoudhury, K. Narayan Kumar, C.R. Ramakrishnan, I.V. Ramakrishnan and Scott A. Smolka</i>	
Abstracting WS1S Systems to Verify Parameterized Networks .....	188
<i>Kai Baukus, Saddek Bensalem, Yassine Lakhnech and Karsten Stahl</i>	
FMona: A Tool for Expressing Validation Techniques over Infinite State Systems .....	204
<i>J.-P. Bodeveix and M. Filali</i>	
Transitive Closures of Regular Relations for Verifying Infinite-State Systems .....	220
<i>Bengt Jonsson and Marcus Nilsson</i>	

## Diagnostic and Test Generation

Using Static Analysis to Improve Automatic Test Generation .....	235
<i>Marius Bozga, Jean-Claude Fernandez and Lucian Ghirvu</i>	
Efficient Diagnostic Generation for Boolean Equation Systems .....	251
<i>Radu Mateescu</i>	

## Efficient Model-Checking

Compositional State Space Generation with Partial Order Reductions for Asynchronous Communicating Systems .....	266
<i>Jean-Pierre Krimm and Laurent Mounier</i>	
Checking for CFFD-Preorder with Tester Processes .....	283
<i>Juhana Helovuo and Antti Valmari</i>	
Fair Bisimulation .....	299
<i>Thomas A. Henzinger and Sriram K. Rajamani</i>	
Integrating Low Level Symmetries into Reachability Analysis .....	315
<i>Karsten Schmidt</i>	

## Model-Checking Tools

Model Checking Support for the ASM High-Level Language .....	331
<i>Giuseppe Del Castillo and Kirsten Winter</i>	

A Markov Chain Model Checker .....	347
<i>Holger Hermanns, Joost-Pieter Katoen, Joachim Meyer-Kayser and Markus Siegle</i>	
Model Checking SDL with Spin .....	363
<i>Dragan Bošnački, Dennis Dams, Leszek Holenderski and Natalia Sidorova</i>	
Salsa: Combining Constraint Solvers with BDDs for Automatic Invariant Checking .....	378
<i>Ramesh Bharadwaj and Steve Sims</i>	

## Symbolic Model-Checking

Symbolic Model Checking of Probabilistic Processes Using MTBDDs and the Kronecker Representation .....	395
<i>Luca de Alfaro, Marta Kwiatkowska, Gethin Norman, David Parker and Roberto Segala</i>	
Symbolic Reachability Analysis Based on SAT-Solvers .....	411
<i>Parosh Aziz Abdulla, Per Bjesse and Niklas Eén</i>	
Symbolic Representation of Upward-Closed Sets .....	426
<i>Giorgio Delzanno and Jean-François Raskin</i>	
BDD vs. Constraint-Based Model Checking: An Experimental Evaluation for Asynchronous Concurrent Systems .....	441
<i>Tevfik Bultan</i>	

## Visual Tools

Tool-Based Specification of Visual Languages and Graphic Editors .....	456
<i>Magnus Niemann and Roswitha Bardohl</i>	
VIP: A Visual Editor and Compiler for v-Promela .....	471
<i>Moataz Kamel and Stefan Leue</i>	

## Verification of Critical Systems

A Comparison of Two Verification Methods for Speculative Instruction Execution .....	487
<i>Tamara Arons and Amir Pnueli</i>	
Partial Order Reductions for Security Protocol Verification .....	503
<i>Edmund Clarke, Somesh Jha and Will Marrero</i>	
Model Checking Security Protocols Using a Logic of Belief .....	519
<i>Massimo Benerecetti and Fausto Giunchiglia</i>	

A Formal Specification and Validation of a Critical System in  
Presence of Byzantine Errors ..... 535  
*S. Gnesi, D. Latella, G. Lenzini, C. Abbaneo, A. Amendola and P. Marmo*

**Author Index** ..... 551