

Ed Brinksma (Ed.)

# Tools and Algorithms for the Construction and Analysis of Systems

Third International Workshop, TACAS'97  
Enschede, The Netherlands, April 2-4, 1997  
Proceedings



Springer

# Lecture Notes in Computer Science

1217

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

Advisory Board: W. Brauer D. Gries J. Stoer

## Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

## Volume Editor

Ed Brinksma

University of Twente, Centre for Telematics and Information Technology

PO Box 217, 7500 AE Enschede, The Netherlands

E-mail: brinksma@cs.utwente.nl

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

**Tools and algorithms for the construction and analysis of systems** : third international workshop ; proceedings / TACAS '97, Enschede, The Netherlands, April 2 - 4, 1997. Ed Brinksma (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1997

(Lecture notes in computer science ; Vol. 1217)

ISBN 3-540-62790-1

NE: Brinksma, Ed [Hrsg.]; TACAS <3, 1997, Enschede>; GT

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

ISSN 0302-9743

ISBN 3-540-62790-1 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 1997

Printed in Germany

Typesetting: Camera-ready by author

SPIN 10549404 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

## Foreword

This volume contains the proceedings of the Third International Workshop on *Tools and Algorithms for the Construction and Analysis of Systems*, TACAS'97, which was held at the University of Twente at Enschede, The Netherlands, April 2–4 1997. Previous workshops took place in Aarhus (1995) and Passau (1996).

It is the goal of the TACAS workshops to bring together researchers and practitioners interested in the development and application of tools and algorithms for the specification, analysis, and construction of information systems. In particular, it aims to create an atmosphere that promotes a cross-fertilization of ideas between the different communities of theorists, tool-builders, tool-users, and system designers in various specialist areas of computer science. Therefore, in addition to the more or less standard criteria for acceptability, contributions have also been selected on the basis of their conceptual significance to neighbouring areas of specialization. In order to emphasize the practical importance of tools, TACAS allows tool demonstrations to be submitted (and reviewed) on an 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 workshop, of course, also organized demonstrations of tools that were not part of the official programme.

In addition to 20 regular papers and 5 tool demonstrations that had been selected out of 54 submissions, the programme of TACAS'97 included invited lectures by three renowned scientists:

- Gérard Berry, Ecole des Mines de Paris and INRIA, Sophia-Antipolis, France, on *Hardware and Software Synthesis from Esterel Programs*,
- Kurt Jensen, University of Aarhus, Denmark, on *Coloured Petri Nets*,
- Zohar Manna, Stanford University, USA, on *Visual Verification*.

TACAS'97 also featured a satellite meeting, viz. the SPIN'97 workshop. This workshop was held at the University of Twente at Enschede following TACAS'97, on April 5, 1997. The SPIN workshops are a meeting point for the international community of users of the SPIN model checking tool.

TACAS'97 was hosted and supported by the University of Twente and its research institute, the Centre for Tele-Informatics and Information Technology. It was sponsored by the Dutch National Graduate School IPA (Institute for Programming research and Algorithmics), CMG, and Siemens-Nixdorf. TACAS'98 will be held in Lisbon as part of the new, confederated European Conference of Theory and Practice of Software, ETAPS'98.

Last, but not least, I would like to thank the TACAS'97 Programme Committee and all the referees, who assisted in the selection of the papers and tool demonstrations. On the local level I would like to thank the University Board for their

ample support, and Pedro D'Argenio, Joke Lammerink, Rom Langerak, and Albert Nijmeijer for all their assistance with the organization of the workshop. Without their hard work TACAS'97 would not have been possible.

April 1997

Ed Brinksma

## Programme Committee

Ed Brinksma (Chair) (NL)	Eric Madelaine (F)
Rance Cleaveland (USA)	Tom Melham (UK)
Loe Feijs (NL)	Alan Mycroft (UK)
Susanne Graf (F)	Scott Smolka (USA)
Gerard Holzmann (USA)	Bernhard Steffen (D)
Kim G. Larsen (DK)	Wolfgang Thomas (D)
Nancy Leveson (USA)	Frits Vaandrager (NL)

## Referees

L. Aceto	Daniel Hirschkoff	Catherine Parent
Charles Andre	Jozef Hooman	Paola Quaglia
Twan Basten	Hans Huttel	Stefan Römer
Michael von der Beeck	Anna Ingolfssdottir	Pascal Raymond
Karen Bernstein	Claude Jard	Judi Romijn
Nikolaj S. Bjørner	Roel de Jong	Oliver Ruething
Doeko Bosscher	Hans Jonkers	Theo C. Ruys
Amar Bouali	Thierry Jron	Hassen Saidi
Frederic Boussinot	Joost-Pieter Katoen	Davide Sangiorgi
Tineke de Bunje	Peter Kelb	Roberto Segala
Pedro R. D'Argenio	Alain Kerbrat	Helmut Seidl
Dennis Dams	Ralf Klasing	R. de Simone
Philippe Darondeau	Bart Knaack	Satnam Singh
Thierry Despeyroux	Kaare J. Kristoffersen	Arne Skou
Marco Devillers	Peter Ladkin	Konrad Slind
Yifei Dong	Rom Langerak	Jan Springintveld
Xiaoqun Du	J.M. Leon	Laurent Thery
K. Engelhardt	Xinxin Liu	P.S. Thiagarajan
Rob Gerth	G. Luetzgen	Chris Tofts
Rob van Glabbeek	Markus Müller-Olm	Jan Tretmans
Stefania Gnesi	Florence Maraninchi	Rob Udink
Patrice Godefroid	Tiziana Margaria	Tomas E. Uribe
Georges Gonthier	Sjouke Mauw	Antti Valmari
Sergei Gorlatch	Stephan Melzer	Carsten Weise
David Griffioen	Michael Mendler	Thomas Wilke
Peter Habermehl	Faron Moller	Sergio Yovine
Klaus Havelund	Jean Moonen	Eduard G. Zondag
J. Hedegaard Andersen	Brian Nielsen	
Lex Heerink	Albert Nymeyer	

# Contents

## Session 1: Invited Talk

Hardware and Software Synthesis, Optimization, and Verification from Esterel Programs .....	1
<i>Gérard Berry</i>	

## Session 2: Space Reduction Techniques

Manipulation Algorithms for K*BMDs .....	4
<i>R. Drechsler, B. Becker, S. Ruppertz</i>	
Combining Partial Order and Symmetry Reductions.....	19
<i>E.A. Emerson, S. Jha, D. Peled</i>	
Partial Model Checking with ROBDDs.....	35
<i>H.R. Andersen, J. Staunstrup, N. Maretti</i>	
Space Efficient Reachability Analysis Through Use of Pseudo-Root States .....	50
<i>A.N. Parashkevov, J. Yantchev</i>	

## Session 3: Tool Demonstrations

The Reference Component of PEP .....	65
<i>B. Grahlmann</i>	
A Tool to Support Formal Reasoning about Computer Languages .....	81
<i>R.J. Boulton</i>	
The Term Processor Generator Kimwitu .....	96
<i>P. van Eijk, A. Belinfante, H. Eertink, H. Alblas</i>	
Graphs in METAFame: The Unifying Power of Polymorphism.....	112
<i>M. von der Beeck, V. Braun, A. Claßen, A. Dannecker, C. Friedrich, D. Koschützki, T. Margaria, F. Schreiber, B. Steffen</i>	

## Session 4: Logical Techniques

A Tableau System for Linear-TIME Temporal Logic .....	130
<i>P.H. Schmitt, J. Goubault-Larrecq</i>	
Model-Checking for a Subclass of Event Structures.....	145
<i>W. Penczek</i>	
Real-Time Logics: Fictitious Clock as an Abstraction of Dense Time ....	165
<i>J.-F. Raskin, P.-Y. Schobbens</i>	
MOSEL: A Flexible Toolset for Monadic Second-Order Logic.....	183
<i>P. Kelb, T. Margaria, M. Mendler, C. Gsottberger</i>	

## Session 5: Invited Talk

A Brief Introduction to Coloured Petri Nets.....	203
<i>Kurt Jensen</i>	

Design/CPN – A Computer Tool for Coloured Petri Nets .....	209
<i>S. Christensen, J.B. Jørgensen, L.M. Kristensen</i>	
<b>Session 6: Verification Support</b>	
Formal Verification of Statecharts with Instantaneous Chain	
Reactions .....	224
<i>J. Philipps, P. Scholz</i>	
Compositional State Space Generation from Lotos Programs .....	239
<i>J.-P. Krimm, L. Mounier</i>	
Syntactic Detection of Process Divergence and Non-local	
Choice in Message Sequence Charts.....	259
<i>H. Ben-Abdallah, S. Leue</i>	
An Automata Based Verification Environment for Mobile Processes .....	275
<i>G. Ferrari, G. Ferro, S. Gnesi, U. Montanari, M. Pistore, G. Ristori</i>	
<b>Session 7: Specification and Analysis</b>	
Compositional Performance Analysis.....	290
<i>C. Tofts</i>	
Incremental Development of Deadlock-Free Communicating Systems.....	306
<i>S. Kleuker</i>	
Automatic Synthesis of Specifications from the Dynamic	
Observation of Reactive Programs .....	321
<i>B. Boigelot, P. Godefroid</i>	
<b>Session 8: Invited Talk</b>	
Visual Verification of Reactive Systems .....	334
<i>Luca de Alfaro, Zohar Manna, Henny B. Sipma, Tomás E. Uribe</i>	
<b>Session 9: Theorem Proving, Model Checking and Their Applications</b>	
Theorem Prover Support for the Refinement of Stream Processing	
Functions .....	351
<i>R. Sandner, O. Müller</i>	
Integration in PVS: Tables, Types, and Model Checking.....	366
<i>S. Owre, J. Rushby, N. Shankar</i>	
Test Generation for Intelligent Networks Using Model Checking .....	384
<i>A. Engels, L. Feijs, S. Mauw</i>	
Mechanically Verified Self-Stabilizing Hierarchical Algorithms .....	399
<i>I.S.W.B. Prasetya</i>	
The Bounded Retransmission Protocol Must Be on Time! .....	416
<i>P.R. D'Argenio, J.-P. Katoen, T.C. Ruys, J. Tretmans</i>	
Author Index.....	433