

Lecture Notes in Computer Science

939

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

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

Pierre Wolper (Ed.)

Computer Aided Verification

7th International Conference, CAV '95
Liège, Belgium, July 3-5, 1995
Proceedings



Springer

Series Editors

Gerhard Goos

Universität Karlsruhe

Vincenz-Priessnitz-Straße 3, D-76128 Karlsruhe, Germany

Juris Hartmanis

Department of Computer Science, Cornell University

4130 Upson Hall, Ithaca, NY 14853, USA

Jan van Leeuwen

Department of Computer Science, Utrecht University

Padualaan 14, 3584 CH Utrecht, The Netherlands

Volume Editor

Pierre Wolper

Institut d'Electricité Montefiore, Université de Liège

Sart Tilman, B28, B-4000 Liège, Belgium

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Computer aided verification : 7th international workshop ;
proceedings / CAV '95, Liège, Belgium, July 3 - 5, 1995. Pierre
Wolper (ed.). - Berlin ; Heidelberg ; New York : Springer, 1995
(Lecture notes in computer science ; Vol. 939)

ISBN 3-540-60045-0

NE: Wolper, Pierre [Hrsg.]; CAV <7, 1995, Liège>; GT

CR Subject Classification (1991): F3, D.2.4, D.2.2, F4.1, B.7.2, C.3, I.2.3

ISBN 3-540-60045-0 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 1995

Printed in Germany

Typesetting: Camera-ready by author

SPIN: 10486339 06/3142 - 543210 - Printed on acid-free paper

Preface

This volume contains the proceedings of the Seventh Conference on Computer Aided Verification (CAV'95), held in Liège, Belgium, on July 3-5, 1995.

The objective of the CAV conferences is to bring together researchers and practitioners who are interested in the theory and practice of computer-assisted formal verification. Though originally oriented towards finite-state concurrent systems, CAV covers all styles of verification approaches and a variety of application areas. The contributions presented at CAV range from theory to concrete applications, but its emphasis is on verification tools and the algorithms and techniques that are needed for their implementation.

Of the 77 papers submitted this year, 31 were accepted for presentation. Invited talks were given by R. Bryant (Carnegie-Mellon University), P. Cousot (Ecole Normale Supérieure, Paris), and E. A. Emerson (University of Texas, Austin). The trend to generalize beyond finite-state systems has definitely continued this year as witnessed by the contributions on general symbolic approaches, on the use of abstraction, and on theorem-proving based approaches. Real-time and hybrid systems are still an important part of the conference. Also, several papers are devoted to the problem of synthesizing (rather than verifying) a concurrent module. Finally, papers describing applications, tools, or experiments are well represented in the conference.

The program committee was very active in reviewing the papers and shaping the final program. This year the program committee members were R. Alur (AT&T Bell Labs, USA), R. Brayton (U. of California, Berkeley, USA), C. Courcoubetis (U. of Crete & ICS-FORTH, Greece), W. Damm (C. v. Ossietzki U., Oldenburg, Germany), R. de Simone (INRIA, Sophia-Antipolis, France), R. Devillers (Free U. of Brussels, Belgium), E. Allen Emerson (U. of Texas, USA), S. Garland (MIT, USA), O. Grumberg (Technion, Israel), N. Halbwachs (VERIMAG, France), T. Henzinger (Cornell U., USA), R. Koymans (Philips Res. Labs, The Netherlands), G. Leduc (U. of Liège, Belgium), K. McMillan (Cadence Berkeley Labs, USA), J. Parrow (SICS, Sweden), N. Shankar (SRI International, USA), F. Somenzi (U. of Colorado, Boulder, USA), B. Steffen (U. of Passau, Germany), P. Varaiya (U. of California, Berkeley, USA), M. Vardi (Rice U., USA), and T. Yoneda (Tokyo Inst. of Technology, Japan).

The Program Committee Chair and General Chair of the conference was Pierre Wolper of the University of Liège. Last year's Program and General Chair D. Dill (Stanford U., USA), as well as the Steering Committee consisting of the conference founders E. Clarke (Carnegie Mellon U., USA), R. Kurshan (AT&T Bell Labs, USA), A. Pnueli (Weizmann Inst., Israel), and J. Sifakis (VERIMAG, France) provided valuable advice on the organization of the conference.

Financial support was provided by the Belgian National Fund for Scientific Research (F.N.R.S.), the government of the "Communauté Française de Belgique", and the University of Liège. Local arrangements were organized by the A.I.M. (Association des Ingénieurs de l'Institut Montefiore) under the supervi-

sion of Ch. Lacrosse. Secretarial assistance was provided by M. Gengler. The handling of the electronic submissions and the preparation of the final camera-ready copy of the proceedings were done by B. Boigelot and Ph. Lejoly.

Finally, the following people helped by evaluating one or more papers: R. Amadio, A. Anuchitanukul, P. Attie, A. Aziz, J. Baeten, S. Bensalem, A. Bouali, O. Burkart, K. Cerans, R. Cleaveland, P. Collette, D. Cyrluk, M. Dam, T. de Bunje, R. de Jong, G. Doehmen, C. Eisner, L.-H. Eriksson, L. Feijs, J.-C. Fernandez, L. Fix, Xavier Fornari, L.-å. Fredlund, J. F. Groote, R. Gerth, A. Geser, A. Girault, P. Godefroid, P. Gribomont, D. Griffioen, K. Hamaguchi, H. Hiraishi, P.-H. Ho, R. Hojati, J. Hooman, M. Hultström, H. Hungar, P. Jancar, H. Jonkers, B. Josko, M. Kaltenbach, T. Kam, M. Kaminski, S. Katz, P. Kopke, F. Korf, S. Krishnan, Y. Kukimoto, R. Kumar, O. Kupferman (Bernholtz), M. Lara de Souza, L. Leonard, H. Lin, G. Luetzgen, E. Madelaine, J.-C. Madre, J. Makowski, O. Maler, T. Margaria, T. Minohara, F. Moller, K. Namjoshi, K. Namjoshi, F. Orava, C. Pecheur, D. Peled, O. Ploton, S. Rajan, R. Ranjan, P. Raymond, R. Robbana, J. Rushby, M. Saarepera, D. Sangiorgi, H. Schepers, H. Schlingloff, R. Schlör, T. Shiple, V. Singhal, P. Sistla, G. Swamy, S. T. Cheng, A. Takahara, S. Tasiran, W. Thomas, R. Trefler, L. Tumlin, F. Vaandrager, C. Weise, H. Wong-Toi, M. Yoeli, S. Yovine, E. Zondag.

Liège, April 1995

Pierre Wolper

Table of Contents

Session 1: Invited Talk

Multipliers and Dividers: Insights on Arithmetic Circuit Verification <i>R. E. Bryant</i>	1
--	---

Session 2

Global Rebuilding of OBDD's - Avoiding Memory Requirement Maxima <i>J. Bern, C. Meinel and A. Slobodová</i>	4
Generating BDD Models for Process Algebra Terms <i>A. Dsouza and B. Bloom</i>	16
Hardware Verification Using Monadic Second-Order Logic <i>D. A. Basin and N. Klarlund</i>	31
Verifying Safety Properties of a Class of Infinite-State Distributed Algorithms <i>B. Jonsson and L. Kempe</i>	42

Session 3

Model Checking for Infinite State Systems Using Data Abstraction, Assumption-Commitment Style Reasoning and Theorem Proving <i>J. Dingel and T. Filkorn</i>	54
CAVEAT: Technique and Tool for Computer Aided VERification and Transformation <i>E. P. Gribomont and D. Rossetto</i>	70
An Integration of Model Checking with Automated Proof Checking <i>S. Rajan, N. Shankar and M. K. Srivas</i>	84

Session 4

Automatic Datapath Abstraction in Hardware Systems <i>R. Hojati and R. K. Brayton</i>	98
--	----

Toupie = μ -Calculus + Constraints

A. Rauzy 114

Safety Property Verification of Esterel Programs and Applications to
Telecommunications Software

L. J. Jagadeesan, C. Puchol and J. E. Von Olnhausen 127

Session 5: Invited Tutorial

Methods for μ -Calculus Model Checking

E. A. Emerson 141

Session 6

Efficient Checking of Behavioural Relations and Modal Assertions Using
Fixed-Point Inversion

H. R. Andersen and B. Vergauwen 142

It Usually Works: The Temporal Logic of Stochastic Systems

A. Aziz, V. Singhal, F. Balarin, R. K. Brayton and

A. L. Sangiovanni-Vincentelli 155

Local Liveness for Compositional Modeling of Fair Reactive Systems

R. Alur and T. A. Henzinger 166

Trace Theoretic Verification of Asynchronous Circuits Using Unfoldings

K. L. McMillan 180

Session 7

From Duration Calculus to Linear Hybrid Automata

A. Bouajjani, Y. Lakhnech and R. Robbana 196

Local Model Checking for Real-Time Systems

O. V. Sokolsky and S. A. Smolka 211

Algorithmic Analysis of Nonlinear Hybrid Systems

T. A. Henzinger and P.-H. Ho 225

Session 8

On Polynomial-Size Programs Winning Finite-State Games <i>H. Lescow</i>	239
The Rabin Index and Chain Automata, with Applications to Automata and Games <i>S. C. Krishnan, A. Puri, R. K. Brayton and P. P. Varaiya</i>	253
An Automata-Theoretic Approach to Fair Realizability and Synthesis <i>M. Y. Vardi</i>	267
Supervisory Control of Finite State Machines <i>A. Aziz, F. Balarin, R. K. Brayton, M. D. DiBenedetto, A. Saldanha and A. L. Sangiovanni-Vincentelli</i>	279

Session 9: Invited Talk

Compositional and Inductive Semantic Definitions in Fixpoint, Equa- tional, Constraint, Closure-Condition, Rule-Based and Game-Theoretic Form <i>P. Cousot and R. Cousot</i>	293
---	-----

Session 10

Utilizing Symmetry when Model Checking Under Fairness Assumptions: an Automata-Theoretic Approach <i>E. A. Emerson and A. P. Sistla</i>	309
Augmenting Branching Temporal Logics with Existential Quantification over Atomic Propositions <i>O. Kupferman (Bernholtz)</i>	325
Modelling Asynchrony with a Synchronous Model <i>R. P. Kurshan, M. Merritt, A. Orda and S. R. Sachs</i>	339
On the Model Checking Problem for Branching Time Logics and Basic Parallel Processes <i>J. Esparza and A. Kiehn</i>	353

Session 11

Using Formal Verification/Analysis Methods on the Critical Path in
System Design: A Case Study

A. Th. Eiriksson and K. L. McMillan 367

Automated Analysis of an Audio Control Protocol

P.-H. Ho and H. Wong-Toi 381

Interactively Verifying a Simple Real-Time Scheduler

C. Fidge, P. Kearney and M. Utting 395

Session 12

Verification of Real-Time Systems by Successive Over and Under
Approximation

D. Dill and H. Wong-Toi 409

Efficient Timing Analysis of a Class of Petri Nets

H. Hulgaard and S. M. Burns 423

Verifying ω -Regular Properties for a Subclass of Linear Hybrid Systems

A. Bouajjani and R. Robbana 437

Author Index 451