Lecture Notes in Computer Science 663

G. v. Bochmann D. K. Probst (Eds.)

Computer Aided Verification

Fourth International Workshop, CAV '92
Montreal, Canada, June 29 - July 1, 1992
Proceedings

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Series Editors

Gerhard Goos
Universität Karlsruhe
Postfach 69 80
Vincenz-Priessnitz-Straße 1
W-7500 Karlsruhe, FRG

Juris Hartmanis
Cornell University
Department of Computer Science
4130 Upson Hall
Ithaca, NY 14853, USA

Volume Editors

Gregor von Bochmann
Departement d'IRO, Université de Montreal
P. O. Box 6128, Station A, Montreal, Quebec, H3C 3J7, Canada

David Karl Probst
Department of Computer Science, Concordia University
1455 de Maisonneuve West, Montreal, Quebec, H3G 1M8, Canada

CR Subject Classification (1991): F.3, D.2.4, B.7, C.2.2

ISBN 3-540-56496-9 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-56496-9 Springer-Verlag New York Berlin Heidelberg

Typesetting: Camera ready by author/editor
45/3140-543210 - Printed on acid-free paper

Preface

This is the Proceedings of the Fourth Workshop on Computer-Aided Verification (CAV '92), held in Montreal, June 29 - July 1, 1992. The objective of this series of workshops is to bring together researchers and practitioners interested in the development and use of methods, tools and theories for the computer-aided verification of concurrent systems. The workshops provide an opportunity for comparing various verification methods and practical tools that can be used to assist the applications designer. Emphasis is placed on new research results and the application of existing results to real verification problems.

Of the 75 papers that were submitted, 31 were accepted for presentation. Leslie Lamport gave the invited talk on hierarchical structure in proofs. Amir Pnueli was the banquet speaker. There were sessions devoted to Reduction Techniques, Proof Checking, Symbolic Verification, Timing Verification, Partial-Order Approaches, Case Studies, Model and Proof Checking, and Other Approaches.

Financial support was provided by Concordia University, Computer Research Institute of Montreal (CRIM), Bell Northern Research (BNR), the IDACOM-NSERC-CWARC Industrial Research Chair on Communication Protocols, the Institut National de la Recherche Scientifique (INRS-Telecommunications), the Natural Sciences and Engineering Research Council of Canada (NSERC), and the University of Montreal.

The Program Committee reviewed, managed other reviewers, and helped in the establishment of the program. The Steering Committee, consisting of E.M. Clarke (Carnegie Mellon University), R.P. Kurshan (AT&T Bell Laboratories), A. Pnueli (Weizmann Institute), and J. Sifakis (LGI-IMAG), reviewed and offered council at appropriate moments. This year, the Program Committee members were: R. Alur (AT&T Bell Labs), R. Brayton (UC Berkeley), E. Brinksma (U. Twente), E. Cerny (U. Montreal), C. Courcoubetis (U. Crete), R. de Simone (INRIA), D. Dill (Stanford U.), A. Emerson (UT Austin), O. Grumberg (Technion), H. Hiraishi (Kyoto Sangyo U.), G. Holzmann (AT&T Bell Labs), W.A. Hunt Jr. (CLI), K. Larsen (Aalborg U.), P. Loewenstein (Sun), A. Mazurkiewicz (Polish Acad. Sci.), L. Paulson (Cambridge U.), D.K. Probst (Concordia U.), B. Steffen (TU Aachen), D. Taubner (sd&m GmbH) and P. Wolper (U. Liege). The names of additional reviewers are listed on the following page.

Gregor v. Bochmann was General and Program Chair. David K. Probst was Local Arrangements Chair and much more. Lucie Levesque was Registration Chair and resource person. Anindya Das was Treasurer. Stan Swiercz and Daniel Ouimet provided technical support for tool demonstrations. Most of the articles in this volume were typeset using the LaTeX document preparation system and Springer-Verlag's LNCS style file, slightly modified.

Montreal, January 1993

Gregor v. Bochmann
David K. Probst

Additional Reviewers

P. Attie (UT Austin), A. Aziz (UC Berkeley), W. Baker (UC Berkeley), F. Balarin (UC Berkeley), D. Barnard (TU Munich), H. Baumer (U Twente), R. Bayardo (UT Austin), O. Bernholtz (Technion), A. Borjesson (Aalborg U), B. Botma (U Twente), A. Bouajjani (LGI-IMAG), A. Bouali (INRIA), G. Boudol (INRIA), O. Burkart (RWTH Aachen), I. Castellani (INRIA), A. Claen (RWTH Aachen), H. Eertink (U Twente), P. Eijk (U Twente), U. Engberg (Aarhus U), T. Filkorn (Siemens), N. Francez (Technion), M. Fujita (Fujitsu), H. Garavel (Verilog), P. Godefroid (U Liege), C. Godskesen (Aalborg U), M. Gordon (Cambridge), S. Graf (LGI-IMAG), P. Gutwin (UC Berkeley), N. Halbwachs (LGI-IMAG), K. Hamaguchi (Kyoto U), T. Henzinger (Cornell U), R. Hojati (UC Berkeley), A. Hu (Stanford U), H. Huttel (Aalborg U), C. Jard (IRISA), T. Jeron (Alcatel), C. Jutla (IBM), M. Kaltenbach (UT Austin), T. Kam (UC Berkeley), P. Kars (U Twente), S. Katz (Technion), S. Kimura (Kobe U), A. Kindler (RWTH Aachen), M. Klein (RWTH Aachen), J. Knoop (Kiel), S. Krishnan (UC Berkeley), W. Lam (UC Berkeley), R. Langerak (U Twente), L. Lavagno (UC Berkeley), C. Loiseaux (LGI-IMAG), A. Mader (TU Munich), J. Makowsky (Technion), A. Mendelson (Technion), F. Mignard (INRIA), C. Moon (UC Berkeley), D. Ouimet (U Montreal), R. Rajaraman (UT Austin), C. Ratel (LGI-IMAG), D. Russinoff (CLI), S. Sagiv (Haifa), A. Scholz (Siemens), M. Sekine (UC Berkeley), N. Shankar (SRI), T. Shiple (UC Berkeley), M. Sinderen (U Twente), A. Skou (Aalborg U), P. Stephan (UC Berkeley), J. Tretmans (U Twente), F. Vaandrager (INRIA), J. Vaucher (U Montreal), T. Villa (UC Berkeley), H. Wang (UC Berkeley), C. Weise (RWTH Aachen), G. Whitcomb (UC Berkeley), H. Wong-Toi (Stanford U), W. Yi (Aalborg U), M. Yoeli (Technion), G. York (UC Berkeley), S. Yovine (LGI-IMAG).

Table of Contents

Invited Lecture:

Session: Reduction Techniques I

Session: Proof Checking

Session: Symbolic Verification I

Session: Timing Verification I

Session: Partial-Order Approaches

Session: Case Studies

Session: Reduction Techniques II

Session: Timing Verification II

Session: Model and Proof Checking

Session: Other Approaches

Session: Symbolic Verification II