

Lecture Notes in Computer Science

1703

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

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

Laurence Pierre Thomas Kropf (Eds.)

Correct Hardware Design and Verification Methods

10th IFIP WG10.5 Advanced Research
Working Conference, CHARME'99
Bad Herrenalb, Germany, September 27-29, 1999
Proceedings



Springer

Series Editors

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

Volume Editors

Laurence Pierre
CMI/Université de Provence
39, rue Joliot-Curie, F-13453 Marseille Cedex 13, France
E-mail: laurence@gyptis.univ-mrs.fr

Thomas Kropf
Technische Informatik, Universität Tübingen
Im Sand 13, D-72076 Tübingen, Germany
E-mail: kropf@informatik.uni-tuebingen.de

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Correct hardware design and verification methods : 10th IFIP WG
10.5 advanced research working conference ; proceedings / CHARME
'99, Bad Herrenalb, Germany, September 27 - 29, 1999. Pierre
Laurence ; Thomas Kropf (ed.). - Berlin ; Heidelberg ; New York ;
Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo
: Springer, 1999
(Lecture notes in computer science ; Vol. 1703)
ISBN 3-540-66559-5

CR Subject Classification (1998): B, F.3.1, D.2.4, F.4.1, I.2.3, J.6

ISSN 0302-9743

ISBN 3-540-66559-5 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 10704583 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

CHARME'99 is the tenth in a series of working conferences devoted to the development and use of leading-edge formal techniques and tools for the design and verification of hardware and systems. Previous conferences have been held in Darmstadt (1984), Edinburgh (1985), Grenoble (1986), Glasgow (1988), Leuven (1989), Torino (1991), Arles (1993), Frankfurt (1995) and Montreal (1997). This workshop and conference series has been organized in cooperation with IFIP WG 10.5. It is now the biannual counterpart of FMCAD, which takes place every even-numbered year in the USA. The 1999 event took place in Bad Herrenalb, a resort village located in the Black Forest close to the city of Karlsruhe.

The validation of functional and timing behavior is a major bottleneck in current VLSI design systems. A predominantly academic area of study until a few years ago, formal design and verification techniques are now migrating into industrial use. The aim of CHARME'99 is to bring together researchers and users from academia and industry working in this active area of research. Two invited talks illustrate major current trends: the presentation by Gérard Berry (Ecole des Mines de Paris, Sophia-Antipolis, France) is concerned with the use of synchronous languages in circuit design, and the talk given by Peter Jansen (BMW, Munich, Germany) demonstrates an application of formal methods in an industrial environment. The program also includes 20 regular presentations and 12 short presentations/poster exhibitions that have been selected from the 48 submitted papers.

The organizers are grateful to IFIP WG 10.5 for its support and to Intel, Siemens, Synopsys, and Verysys for their financial sponsorship, which considerably eased the organization of the conference. We are indebted to Renate Murr-Grobe and Klaus Schneider for their help in organizing this event, to Jörg Berdux for providing the nice layout of the call for papers, and to Eric Gascard for his technical assistance.

September 1999

Laurence Pierre, Program Chair
Thomas Kropf, Conference Chair
CHARME'99

Organization

CHARME'99 was organized in Bad Herrenalb by the University of Karlsruhe and the University of Tübingen (Germany), with the support of IFIP WG10.5.

Program Committee

Conference Chair: Thomas Kropf (Univ. of Tübingen, Germany)
Program Chair: Laurence Pierre (Univ. de Provence, France)
François Anceau (CNAM, France)
Dominique Borrione (Univ. Grenoble, France)
Albert Camilleri (Hewlett-Packard, USA)
Paolo Camurati (Politecnico di Torino, Italy)
Luc Claesen (IMEC, Belgium)
Eduard Cerny (Univ. de Montreal, Canada)
Werner Damm (Univ. Oldenburg, Germany)
Hans Eveking (T.U. Darmstadt, Germany)
Ganesh Gopalakrishnan (Univ. of Utah, USA)
Mike Gordon (Cambridge Univ., UK)
Werner Grass (Univ. Passau, Germany)
Mark Greenstreet (Univ. BC, Canada)
Warren Hunt (IBM, USA)
Steven Johnson (Indiana Univ., USA)
Ramayya Kumar (Verysys, Germany)
Robert Kurshan (Bell Labs, USA)
Tiziana Margaria (Univ. Dortmund, Germany)
Andrew Martin (Motorola, USA)
Ken McMillan (Cadence Berkeley Labs, USA)
Tom Melham (Univ. Glasgow, UK)
Paolo Prinetto (Politecnico di Torino, Italy)
Rajeev Ranjan (Synopsys, USA)
Mary Sheeran (Chalmers Univ., Sweden)
Jørgen Staunstrup (T.U. of Denmark, Denmark)
Sofiene Tahar (Concordia Univ., Canada)

Referees

Magdy Abadir	Per Bjesse	Eduard Cerny
E.M. Aboulhamid	Dominique Borrione	Koen Claessen
Otmane Ait-Mohamed	Olaf Burkart	Abdelkader Dekdouk
Ken Albin	Albert Camilleri	Stephen A. Edwards
F. Anceau	Paolo Camurati	Hans Eveking

Y. Feng	Steve Johnson	Laurence Pierre
Eric Gascard	Michael Jones	K.S. Prasad
Jens Chr. Godskesen	Jens Knoop	Stefano Quer
Ganesh Gopalakrishnan	R. Kurshan	Sriram K. Rajamani
Mike Gordon	V. Levin	Rajeev K. Ranjan
Werner Grass	Panagiotis Manolios	K. Ravi
Mark Greenstreet	Tiziana Margaria	Sophie Renault
Claudia Gsottberger	Andrew Martin	Jun Sawada
Pei-Hsin Ho	Ken McMillan	Klaus Schneider
Stefan Hoereth	Tom Melham	Ken Scott
Peng Hong	Michael Mandler	Mary Sheeran
Ravi Hosabettu	Marcus Müller-Olm	Tom Shiple
Jin Hou	Ratan Nalumasu	Jørgen Staunstrup
Henrik Hulgaard	K. Namjoshi	Terence Stroup
Warren A. Hunt	Félix Nicoli	Sofiene Tahar
M. Jahanpour	Jean-Luc Paillet	Raimund Ubar

Table of Contents

Invited Talks

Esterel and Jazz : Two Synchronous Languages for Circuit Design	1
<i>Gérard Berry</i>	

Design Process of Embedded Automotive Systems - Using Model Checking for Correct Specifications	2
<i>Peter Jansen</i>	

Proof of Microprocessors

A Proof of Correctness of a Processor Implementing Tomasulo's Algorithm without a Reorder Buffer	8
<i>Ravi Hosabettu, Ganesh Gopalakrishnan, Mandayam Srivas</i>	

Formal Verification of Explicitly Parallel Microprocessors	23
<i>Byron Cook, John Launchbury, John Matthews, Dick Kieburtz</i>	

Superscalar Processor Verification Using Efficient Reductions of the Logic of Equality with Uninterpreted Functions to Propositional Logic	37
<i>Miroslav Velev, Randal Bryant</i>	

Model Checking

Model Checking TLA+ Specifications	54
<i>Yuan Yu, Panagiotis Manolios, Leslie Lamport</i>	

Efficient Decompositional Model-Checking for Regular Timing Diagrams . .	67
<i>Nina Amla, E. Allen Emerson, Kedar S. Namjoshi</i>	

Vacuity Detection in Temporal Model Checking	82
<i>Orna Kupferman, Moshe Vardi</i>	

Formal Methods and Industrial Applications

Using Symbolic Model Checking to Verify the Railway Stations of Hoorn-Kersenboogerd and Heerhugowaard	97
<i>Cindy Eisner</i>	

Practical Application of Formal Verification Techniques on a Frame Mux/Demux Chip from Nortel Semiconductors	110
<i>Y.Xu, E.Cerny, A.Silburt, A.Coady, Y.Liu, P.Pownall</i>	

Efficient Verification of Timed Automata Using Dense and Discrete Time Semantics 125
Marius Bozga, Oded Maler, Stavros Tripakis

Abstraction and Compositional Techniques

From Asymmetry to Full Symmetry: New Techniques for Symmetry Reduction in Model Checking 142
E.Allen Emerson, Richard J. Trefler

Automatic Error Correction of Large Circuits Using Boolean Decomposition and Abstraction 157
Dirk W. Hoffmann, Thomas Kropf

Abstract BDDs: A Technique for Using Abstraction in Model Checking . . . 172
Edmund Clarke, Somesh Jha, Yuan Lu, Dong Wang

Theorem Proving Related Approaches

Formal Synthesis at the Algorithmic Level 187
Christian Blumenröhr, Viktor Sabelfeld

Xs Are for Trajectory Evaluation, Booleans Are for Theorem Proving. 202
Mark Aagaard, Thomas Melham, John O’Leary

Verification of Infinite State Systems by Compositional Model Checking . . 219
K.L.McMillan

Symbolic Simulation/Symbolic Traversal

Formal Verification of Designs with Complex Control by Symbolic Simulation 234
Gerd Ritter, Hans Eueking, Holger Hinrichsen

Hints to Accelerate Symbolic Traversal 250
Kavita Ravi, Fabio Somenzi

Specification Languages and Methodologies

Modeling and Checking Networks of Communicating Real-Time Processes . 265
Jürgen Ruf, Thomas Kropf

”Have I Written Enough Properties?” A Method of Comparison between Specification and Implementation 280
Sagi Katz, Orna Grumberg, Danny Geist

Program Slicing of Hardware Description Languages 298
E.Clarke, M.Fujita, S.P.Rajan, T.Reps, S.Shankar, T.Teitelbaum

Posters

Results of the Verification of a Complex Pipelined Machine Model	313
<i>Jun Sawada, Warren A. Hunt, Jr</i>	
Hazard-Freedom Checking in Speed-Independent Systems	317
<i>Husnu Yenigun, Vladimir Levin, Doron Peled, Peter Beerel</i>	
Yet Another Look at LTL Model Checking	321
<i>Klaus Schneider</i>	
Verification of Finite-State-Machine Refinements Using a Symbolic Methodology	326
<i>Stefan Hendrixx, Luc Claesen</i>	
Refinement and Property Checking in High-Level Synthesis Using Attribute Grammars	330
<i>George Economakos, George Papakonstantinou</i>	
A Systematic Incrementalization Technique and Its Application to Hardware Design	334
<i>Steven Johnson, Yanhong Liu, Yuchen Zhang</i>	
Bisimulation and Model Checking	338
<i>Kathi Fisler, Moshe Y. Vardi</i>	
Circular Compositional Reasoning about Liveness	342
<i>K.L.McMillan</i>	
Symbolic Simulation of Microprocessor Models Using Type Classes in Haskell	346
<i>Nancy A. Day, Jeffrey R. Lewis, Byron Cook</i>	
Exploiting Retiming in a Guided Simulation Based Validation Methodology	350
<i>Aarti Gupta, Pranav Ashar, Sharad Malik</i>	
Fault Models for Embedded Systems	354
<i>Jens Chr. Godskesen</i>	
Validation of Object-Oriented Concurrent Designs by Model Checking	360
<i>Klaus Schneider, Michaela Huhn, George Logothetis</i>	
Author Index	365