Lecture Notes in Computer Science 987
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Paolo E. Camurati Hans Eveking (Eds.)

Correct Hardware Design and Verification Methods

IFIP WG 10.5 Advanced Research
Working Conference, CHARME '95
Frankfurt/Main, Germany, October 2-4, 1995
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Paolo E. Camurati
Politecnico di Torino, Dip. di Automatica e Informatica
Corso Duca degli Abruzzi 24, I-10129 Turin, Italy

Hans Eveking
Fachbereich Informatik, Johann Wolfgang Goethe-Universität
Robert-Mayer-Str. 11-15, D-60054 Frankfurt a.M., Germany

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Correct hardware design and verification methods : IFIP WG 10.5 advanced research working conference ; proceedings / CHARME '95, Frankfurt, Germany, October 2 - 4, 1995. Paolo E. Camurati ; Hans Eveking (ed.). - Berlin ; Heidelberg ; New York : Springer, 1995
(Lecture notes in computer science ; Vol. 987)
ISBN 3-540-60385-9
NE: Camurati, Paolo E. [Hrsg.]; CHARME <8, 1995, Frankfurt, Main>; International Federation for Information Processing / Working Group Very Large Scale Integration; GT

CR Subject Classification (1991): I.2-3, H.2, H.5, E.1-2, I.5-6, J.2

ISBN 3-540-60385-9 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 10485715 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

This volume contains the papers presented at the "Advanced Research Working Conference on Correct HARdware Design MEthodologies" (CHARME'95) held at the Johann Wolfgang Goethe-Universität of Frankfurt (Germany) on October 2-4, 1995. This working conference is the eighth in a series dedicated to the development and use of methods for correct design and verification of electronic systems. Previous conferences were held in Darmstadt (1984), Edinburgh (1985), Grenoble (1986), Glasgow (1988), Leuven (1989), Turin, (1991), and Arles (1993).

Its objective was to bring together researchers interested in formal verification of hardware, providing a forum for presenting theoretical advances and practical applications.

The papers cover the following topics, though the list is not exhaustive: model checking, theorem proving, verified synthesis, process algebras, finite state systems, verification environments, language containment, and VHDL.

The program committee members were: Francois Anceau (BULL, Paris), Dominique Borrione (IMAG, France), Paolo Camurati (Univ. Udine, Italy), Ed Cerny (Univ. Monreal, Canada), Luc Claesen (IMEC, Leuven, Belgium), Ed Clarke (Carnegie Mellon University, USA), Werner Damm (Univ. Oldenburg, Germany), Carlos Delgado Kloos (Univ. Madrid, Spain), Hans Eveking (Univ. Frankfurt, Germany), Werner Grass (Univ. Passau, Germany), George Milne (Univ. of South Australia, Australia), Laurence Pierre (Univ. Provence, France), Paolo Prinetto (Politecnico Torino, Italy), Jorgen Staunstrup (Univ. of Denmark, Lyngby).

Program chair was Paolo Camurati (University of Udine). Organization chair was Hans Eveking (University of Frankfurt).

We would also like to thank the following additional reviewers, who helped in the evaluation process: Michel Allemand, Henrik Reif Andersen, Laurent Arditi, Bachir Berkane, Gerard Berry, Dominique Bolignano, Amar Bouali, P.T. Breuer, Gianpiero Cabodi, Fulvio Corno, David Deharbe, Robert de Simone, Luis Sanchez Fernandez, Sergei Gorlatch, Christian Grobe, Stefan Höreth, Karim Khordoc, Yassine Lakhnech, Luciano Lavagno, Andres Marin Lopez, Enrico Macii, Natividad Martinez, Niels Mellergaard, Michael Mendler, Marius Minea, Matthias Mutz, Jean-Luc Paillet, Stefano Quer, Ellen Sentovich, Robin Sharp, S. Tahar, Christoph Wedler.

Stefan Höreth and Angelika Schifignano assisted in planning the local arrangements.

We are grateful to the Commission of the European Communities DG XIII and to the University of Frankfurt for their support.

July 1995

Paolo Camurati
Hans Eveking

Table of Contents

Model checking

What if model checking must be truly symbolic
H. Hungar, OFFIS Oldenburg, Germany
O. Grumberg, The Technion, Haifa, Israel
W. Damm, Oldenburg Univ., Germany 1

Automatic verification of the SCI cache coherence protocol
U. Stern, D.L. Dill, Stanford Univ., USA 21

Theorem proving

Describing and verifying synchronous circuits with the Boyer-Moore theorem prover
L. Pierre, Marseille Univ., France 35

Problems encountered in the machine-assisted proof of hardware
P. Curzon, Cambridge Univ., UK 56

Formally verified synthesis

Formally embedding existing high level synthesis algorithms
D. Eisenbiegler, R. Kumar,
FZI Karlsruhe, Germany 71

Formal design of a class of computers
L.G. Wang, Edinburgh Univ., UK
M. Mendler, Univ. of Denmark, Denmark 84

Process algebras

Symbolic analysis and verification of CPA descriptions
M.C. McFarland, Boston College, USA
T.J. Kowalski, AT&T Bell Labs. USA 103

A foundation for formal reuse of hardware
A.C.V. de Melo, H. Barringer,
Manchester Univ., UK 124

Finite state systems I

State enumeration with abstract descriptions of state machines
F. Corella, IBM Research, USA
M. Langevin, GMD-SET, Germany
E. Cerny, Z. Zhou, X. Song, Montreal Univ. 146

Transforming boolean relations by symbolic encoding
G. Cabodi, S. Quer, Polit. di Torino, Italy
P. Camurati, Udine Univ., Italy 161

Design error diagnosis in sequential circuits
A. Wahba, D. Borrione, Lab. ARTEMIS-IMAG, Grenoble Univ., France 171

Finite state systems II

Timing analysis of asynchronous circuits using timed automata
O. Maler, Spectre-Verimag, France
A. Pnueli, Weizmann Inst., Israel 189

Improved probabilistic verification by hash compaction
U. Stern, D.L. Dill, Stanford Univ., USA 206

Verification environments

Formal support for the ELLA hardware description language
H. Barringer, G. Gough, Manchester Univ., UK
B. Monahan, Harlequin Ltd., UK
A. Williams, Manchester Univ., UK 225

Verifying hardware components within JACK
R. De Nicola, Rome Univ., Italy
A. Fantechi, S. Gnesi, S. Larosa, G. Ristori, Pisa Univ., Italy . 246

Language containment

Language containment of non-deterministic ω-automata
S. Taşiran, R. Hojati, R.K. Brayton,
Univ. of California, Berkeley, USA 261

A partial-order approach to the verification of concurrent systems: checking liveness properties
D. Bolignano, BULL, France 278

VHDL

Semantics of a verification-oriented subset of VHDL
D. Déharbe, D. Borrione, Lab. ARTEMIS-IMAG, Grenoble Univ., France 293

Reasoning about VHDL using operational and observational semantics
K.G.W. Goossens, Rome Univ., Italy 311

A Symbolic Relation for a Subset of VHDL'87 Descriptions and its Application to Symbolic Model Checking
E. Encrenaz, Lab. MASI/IBP, Paris, France 328