

# Lecture Notes in Computer Science

901

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

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

Ramayya Kumar Thomas Kropf (Eds.)

# Theorem Provers in Circuit Design

Theory, Practice and Experience

Second International Conference, TPCD '94  
Bad Herrenalb, Germany, September 26-28, 1994  
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 Editors

Ramayya Kumar

Forschungszentrum Informatik

Haid-und-Neu-Straße 10-14, D-76131 Karlsruhe, Germany

Thomas Kropf

Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe

Zirkel 2, D-76128 Karlsruhe, Germany

CR Subject Classification (1991): F.4.1, I.2.3, B.1.2

ISBN 3-540-59047-1 Springer-Verlag Berlin Heidelberg New York

CIP data applied for

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: 10485414 45/3140-543210 - Printed on acid-free paper

## Preface

This volume contains the final revised proceedings of the Second International Conference on Theorem Provers in Circuit Design, jointly organized by FZI (Forschungszentrum Informatik), Karlsruhe, and the University of Karlsruhe (Universität Karlsruhe, Institut für Rechnerentwurf und Fehlertoleranz), in cooperation with IFIP (International Federation of Information Processing) Working Group 10.2. The workshop took place in the Treff Hotel, Bad Herrenalb, Germany from 26 to 28 September 1994.

The conference was a sequel to the one held at Nijmegen in June 1992 and provided a forum for discussing the role of theorem provers in the design of digital systems. The topics of interest included original research as well as case studies and other practical experiments with new or established theorem proving tools, including tautology and model checkers.

The field of formal methods in hardware abounds with various kinds of formalisms, each of which have their advantages and disadvantages. Two of the popular theorem provers, with different underlying formalisms, were presented as tutorial talks.

Two invited papers highlighted the use of formal methods in circuit design from an academic and an industrial viewpoint. They were given by Tom Melham (*Inductive Reasoning about Circuit Design*) and Pasupati Subrahmanyam (*Compositionality, Hierarchical Verification and the Principle of Transparency*).

An interesting panel discussion on the *Use of Formal Methods in Industry* was conducted with the following participants: Massimo Bombana, Holger Busch, Alberto Camilleri, Pasupati Subrahmanyam, and John van Tassel.

All submitted research papers were reviewed by at least three independent reviewers, who are all experts in the field. The emphasis of the conference was laid on an in-depth presentation of the approaches instead of accepting many papers, hence only 50% of the submitted papers were accepted as full papers, each of which was given 40 minutes of presentation time. Four papers were acknowledged for their interesting ideas and accepted as short papers.

The research papers were complemented by the demonstration of verification systems — *Fancy*, *MEPHISTO*, *PVS*, *Prevail*, and *Synchronized Transitions*.

At this conference also a set of benchmark circuits for hardware-verification was presented. These circuits are the basis for an international standardization effort of IFIP WG10.2 in order to provide a common basis for evaluating and comparing different approaches of hardware verification and formal synthesis.

We thank all people who actively supported us in organizing this conference, all members of the programme committee, and especially Hilke Kloss for solving many organizational details and Frank Imhoff and Dirk Eisenbiegler for their work in setting up the hardware for the system demonstrations. We are also grateful to Michael Berthold for his help in publishing these proceedings.

## **Programme Committee**

Dominique Borrione (IMAG, France)  
 Holger Busch (Siemens AG, Germany)  
 Luc Claesen (IMEC, Belgium)  
 David Dill (Stanford University, USA)  
 Hans Eweking (University of Frankfurt, Germany)  
 Simon Finn (Abstract Hardware Ltd., UK)  
 Mike Gordon (University of Cambridge, UK)  
 Warren A. Hunt Jr. (CL Inc., USA)  
 Paul Loewenstein (Sun, USA)  
 Miriam Leeser (Cornell University, USA)  
 Tom Melham (University of Glasgow, UK)  
 Tobias Nipkow (TU München, Germany)  
 Jørgen Staunstrup (Lyngby University, Denmark)  
 Victoria Stavridou (University of London, UK)  
 Pasupati Subrahmanyam (AT&T Bell Labs, USA)

## **Conference Organization**

### **Conference Chair**

Ramayya Kumar  
 Forschungszentrum Informatik  
 Haid-und-Neu Strasse 10-14  
 D-76131 Karlsruhe  
 Germany

### **Conference Co-Chair**

Thomas Kropf  
 Institut für Rechnerentwurf und Fehlertoleranz  
 Universität Karlsruhe  
 Zirkel 2  
 D-76128 Karlsruhe  
 Germany

### **Local Arrangements**

Hilke Kloss  
 Forschungszentrum Informatik  
 Haid-und-Neu Strasse 10-14  
 D-76131 Karlsruhe  
 Germany

### **Technical Arrangements**

Frank Imhoff  
 Institut für Rechnerentwurf und Fehlertoleranz  
 Universität Karlsruhe  
 Zirkel 2  
 D-76128 Karlsruhe  
 Germany

# Contents

Benchmark-Circuits for Hardware-Verification .....	1
<i>Thomas Kropf</i>	
<b>Research Papers</b>	
Reasoning About Pipelines with Structural Hazards.....	13
<i>Mark Aagaard and Miriam Leeser</i>	
A Correctness Model for Pipelined Microprocessors.....	33
<i>Phillip J. Windley and Michael L. Coe</i>	
Non-Restoring Integer Square Root: A Case Study in Design by Principled Optimization .....	52
<i>John O'Leary, Miriam Leeser, Jason Hickey and Mark Aagaard</i>	
An Automatic Generalization Method for the Inductive Proof of Replicated and Parallel Architectures .....	72
<i>Laurence Pierre</i>	
A Compositional Circuit Model and Verification by Composition .....	92
<i>Zheng Zhu</i>	
Exploiting Structural Similarities in a BDD-Based Verification Method.....	110
<i>C.A.J. van Eijk and G.L.J.M. Janssen</i>	
Studies of the Single Pulser in Various Reasoning Systems .....	126
<i>Steven D. Johnson, Paul S. Miner and Albert Camilleri</i>	
Mechanized Verification of Speed-independence.....	146
<i>Michael Kishinevsky and Jørgen Staunstrup</i>	
Automatic Correctness Proof of the Implementation of Synchronous Sequential Circuits Using an Algebraic Approach .....	165
<i>Junji Kitamichi, Sumio Morioka, Teruo Higashino and Kenichi Taniguchi</i>	
Mechanized Verification of Refinement .....	185
<i>Niels Maretti</i>	
Effective Theorem Proving for Hardware Verification.....	203
<i>D. Cyrluk, S. Rajan, N. Shankar and M.K.Srivas</i>	
A Formal Framework for High Level Synthesis .....	223
<i>Thomas Kropf, Klaus Schneider and Ramayya Kumar</i>	
<b>Tutorial Papers</b>	
Tutorial on Design Verification with Synchronized Transitions.....	239
<i>Niels Møllergaard and Jørgen Staunstrup</i>	

A Tutorial on Using PVS for Hardware Verification .....	258
<i>S. Owre, J.M. Rushby, N. Shankar and M.K. Srivas</i>	

### **Short Papers**

A Reduced Instruction Set Proof Environment .....	280
<i>Holger Busch</i>	
Quantitative Evaluation of Formal Based Synthesis in ASIC Design.....	286
<i>G. Bezzi, M. Bombana, P. Cavalloro, S. Conigliaro and G. Zaza</i>	
Formal Verification of Characteristic Properties .....	292
<i>Michel Allemand</i>	
Extending Formal Reasoning with Support for Hardware Diagrams.....	298
<i>Kathi Fisler</i>	