FORMAL VLSI CORRECTNESS VERIFICATION

VLSI Design Methods-II

FORMAL VLSI CORRECTNESS VERIFICATION

VLSI Design Methods-II

Proceedings of the IFIP WG 10.2/WG 10.5 International Workshop on
Applied Formal Methods for Correct VLSI Design
Sponsored by IMEC, Houthalen, Belgium, 13–16 November, 1989

Edited by

LUC J.M. CLAESEN
Interuniversity Micro-Electronics Center
& Katholieke Universiteit Leuven
Leuven, Belgium

1990

NORTH-HOLLAND
AMSTERDAM · NEW YORK · OXFORD · TOKYO

ELSEVIER SCIENCE PUBLISHERS B.V.
Sara Burgerhartstraat 25
P.O. Box 211, 1000 AE Amsterdam, The Netherlands

Distributors for the United States and Canada:
ELSEVIER SCIENCE PUBLISHING COMPANY INC.
655 Avenue of the Americas
New York, N.Y. 10010, U.S.A.

Library of Congress Cataloging-in-Publication Data

IFIP WG 10.2/WG 10.5 International Workshop on Applied Formal Methods for Correct VLSI Design (1989 : Houthalen, Belgium)
Formal VLSI correctness verification : VLSI Design methods, II : proceedings of the IFIP WG 10.2/WG 10.5 International Workshop on Applied Formal Methods for Correct VLSI Design / sponsored by IMEC, Houthalen, Belgium, 13-16 November, 1989 : edited by Luc J.M. Claesen.
p. cm.
Includes bibliographical references.
ISBN 0-444-88688-5 (U.S.)
1. Integrated circuits--Very large scale integration--Design and construction--Data processing--Congresses. 2. Computer-aided design--Congresses. 3. Integrated circuits--Very large scale integration--Testing--Congresses. I. Claesen, Luc J.M. II. Interuniversity Micro-Electronics Center. · III. Title.
TK7874.I3283 1989a
621.39'5--dc20 90-6949
CIP

ISBN Part 2: 0 444 88688 5

ISBN Part 1: 0 444 88372 X
ISBN Set : 0 444 88689 3

No responsibility is assumed by the publisher or by IFIP for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.

Printed in The Netherlands.

Preface

Applied Formal Methods For Correct VLSI Design.

The international workshop entitled *"Applied Formal Methods For Correct VLSI Design"* has been organized by IMEC, the Interuniversity Micro Electronics Center in Leuven (Belgium), in cooperation with IFIP (International Federation for Information Processing) working group 10.2 *"System Description and Design Tools"* and working group 10.5 *"Very Large Scale Integration"*. The workshop took place in the "Hengelhoef" Congress Village in Houthalen Belgium from 13 to 16 November 1989. The workshop has been followed by a visit to IMEC on 17 November 1989.

Functional and behavioral verification of the correctness, is the bottleneck in current VLSI design systems. For economical reasons, designs of VLSI circuits must be completely validated before manufacturing. Current VLSI validation is mainly done through extensive simulation. The emerging alternative is based on formal design and verification methods, that guarantee correctness.

At this workshop, researchers interested in formal hardware design methods that are applicable for correct VLSI design, from both industries and universities, have been brought together: Invited overview speaches, regular presentations and a poster session on recent research achievements, as well as several demonstrations of CAD-tools making use of formal methods have been organized.

The workshop has been attended by 180 participants from 18 different countries in America, Asia and Europe.

Two invited speaches have been given by prof. Randal E. Bryant *(Symbolic Analysis and Verification of MOS Circuits.)* and by prof. Warren Hunt Jr. *(The Formal Design and Verification of Hardware Based on the Boyer-Moore prover.).*

In response to the *call for papers* 95 contributions have been received. Every contribution has been reviewed by three independent reviewers who have given their opinion on the suitability of the proposed topics for the focus of this workshop. From these, 30 have been selected for presentation in the regular sessions and 20 have been presented in a poster session.

I hereby want to thank the reviewers for their careful reviews and for the return of the review reports in time, taking into account the holiday period in which the reviews had to be carried out. The selection process has been guided by the overall recommendations of the reviewers.

The emphasis has been put on "applied" methods, methods that are illustrated with realistic design problems, methods that have large potential future application to large VLSI design, methods that are implemented in software prototypes, original and high quality contributions. Special attention has also been given to contributions that relate their work to the benchmarks that have been distributed.

Benchmark Examples.

In order to be able to compare and illustrate specific aspects of formal design systems, a set of benchmarks for formal verification and design between RTL specification and hardware implementation have been made available to interested participants.

The first common application is the design of a "Min-Max"-block[1] which has been distributed to illustrate a specific design method or formalism. The main emphasis, with the "Min-Max" application, is on using a common known problem to be used to explain specific approaches, and not so much on the complexity of the problem.

The second class of applications consists of a number of benchmarks[2] for tautology checkers as are often available in formal verification systems. These two benchmark types have been the subject of special sessions.

Demonstration Sessions

In this conference on "*Applied* Formal Methods For Correct VLSI Design" special attention has been given to demonstrations of CAD tools and prototype tools that illustrate recent research results and/or original realizations in the area of formal hardware design and verification methods. During the workshop computer workstations have been made available to the participants for demonstrations to be organized on an individual basis during free time.

Besides the continuous possibility for demonstrations, specific sessions have been organized every day from the second day on. Each demonstration session had a number of prepared demonstrations, together with a short introduction to the demonstration on posters and/or transparancies. The participants have been subdivided in groups and were able to visit all the demonstrations in a synchronized way. There have been presented 25 operational demonstrations in these sessions.

"Organized demonstrations" in special sessions is probably a new event on conferences, and requires more involvement and preparation of the presenters. The concept has been received very well by the participants. I hereby want to thank all of the participants that have presented and prepared for these demonstrations. Special thanks go to Diederik Verkest, who carefully

[1] see: D. Verkest, L. Claesen, H. De Man, "Special Benchmark Session on Formal System Design", in *Formal VLSI Specification and Synthesis*, edited by L. Claesen, North-Holland Publ. 1990.

[2] see: D. Verkest, L. Claesen "Special Benchmark Session on Tautology Checking", in *Formal VLSI Correctness Verification*, edited by L. Claesen, North-Holland Publ. 1990.

did the special arrangements and the intensive preparatory work for the successful organization of the demonstrations.

About this book: Formal VLSI Correctness Verification.

The participants proceedings for the workshop on "Applied Formal Methods For Correct VLSI Design" contained the papers in the order of the presentations. For the final version of the proceedings the decision has been made to split the topics in two parts, that are the subjects of two books published by Elsevier North-Holland Publ.:

1. Formal VLSI Specification and Synthesis.
2. Formal VLSI Correctness Verification.

The subdivision of the two topics is mainly based on a top-down (synthesis) and bottom-up (verification) approaches in VLSI design and verification.

Formal VLSI Specification and Synthesis concentrates on specification formalisms and constructive design methods that guarantee correctness of what is being designed. The papers focus either on transformational or guided synthesis design methods that start from a specification and transform the specification into implementations in a correct way. General theorem prover based methodologies, as well as dedicated algorithms for the design of regular array structures are presented.

Formal VLSI Correctness Verification highlights the methodologies for verifying the correctness of design implementations in a bottom-up way. Abstraction levels from transistor level, over sequential machines and register transfer level are presented. Á specific chapter on tautology checking presents, using the same benchmarks, efficiency comparisons of eight different methods for tautology checking. Boyer-Moore and HOL theorem prover based hardware verification methods are the subject of the last two chapters.

Acknowledgements.

To conclude I want to thank everyone who has contributed to the succes of the *Applied Formal Methods For Correct VLSI Design* workshop: the paper contributors, the program committee, the local organizing committee, the sponsors, the reviewers, the participants, the IFIP WG 10.2 and 10.5 members and many others. Finally I want to give special thanks to prof. Hugo De Man and prof. Roger Van Overstraeten, for their stimulation and support in the organization of this international conference within the scope of IMEC.

Luc J.M. Claesen

Conference organization.

Workshop Organizer:

Luc Claesen
Interuniversity Micro Electronics Center
& Katholieke Universiteit Leuven
Kapeldreef 75,
B-3030 Leuven (Belgium)
e-mail: claesen@imec.be

Program Committee

Francois Anceau (Bull)
Dominique Borrione (IMAG)
Randy Bryant (Carnegie Mellon Univ.)
Luc Claesen (IMEC)
Ed Clarke (Carnegie Mellon Univ.)
Hans Eveking (Techn Hochshule Darmstadt)
Mike Gordon (Univ. of Cambridge)
Warren Hunt (Computational Logic Inc.)
George Milne (Strathclyde Univ.)
Paolo Prinetto (Politecnico di Torino)
P.A. Subrahmanyam (AT&T Holmdell)

Local Organization Committee.

Luc Claesen
Catia Angelo Marcondes
Kris Croes
Hans De Keulenaer
Peter De Vijt
Mark Genoe
Peter Johannes
Wim Ploegaerts
Milton Sawasaki
Robert Severyns
Annemie Stas
Diederik Verkest

Sponsoring and Support

The generous sponsoring by the following organizations is greatfully acknowledged:

Alcatel Bell
Apollo Computer & Hewlett-Packard
I.B.M. Belgium
Mentor Graphics
SUN Microsystems

The following computer manufacturers are acknowledged for making available computer equipement for the demonstrations during the workshop:

Apollo Computer
Digital Equipment Corporation
Hewlett-Packard
SUN Microsystems

IFIP WG10.5 Representative

Eric Schutz

Reviewers

V. Akella
F. Anceau
D. Beatty
J. Benkoski
C. Berthet
I. Bolsens
G. Borriello
D. Borrione
R. Boute
D. Brand
R. Bryant
J. Bu
H. Cai
P. Camurati
F. Catthoor
L. Claesen
E. Clarke
M. Dagenais
J. Darringer
P. Das
C. Delgado Kloos
G. De Michelli
E. De Prettere
D. Dill
N. Dutt
M. Elmasry
H. Eveking
A. Fisher
M. Fourman
D. Gajski
W. Grass
P. Gribomont
M. Gordon
G. Gopalakrishnan

I. Hajj
K. Hanna
R. Hartenstein
W. Hunt
G. Janssen
J. Jess
P. Johannes
A. Kalker
T. Krol
M. Leeser
W. Luk
A. Martin
F. Mavaddat
G. Milne
R. Nair
J.-L. Paillet
S. Perremans
L. Pierre
W. Ploegaerts
P. Prinetto
C. Pygott
A. Salem
C.-J. Seger
Y. Shiran
J. Staunstrup
R. Spickelmeir
P. Subrahmanyam
R. Tjarnstrom
P. Van Bekbergen
C. Van Berkel
V. Van Dongen
J. Van Sas
D. Verkest
J. Zegers

Demonstrations at the workshop.

"LOVERT, VERTICO"
A.Bartsch, H.Eveking, H.-J. Faerber, J. Pinder, U.Schellin, T. H. Darmstadt
"Using TACHE for proving circuits."
C. Bayol, J-L. Paillet, Univ de Provence
"STAT!"
J.Benkoski, M.Chew, A.Strojwas, Carnegie Mellon Univ.
"System SWIVER for verifying asynchronous circuits."
E.Cerny, P.Rioux, C.Berthet, Univ de Montreal
"CATHEDRAL-II"
H.De Keulenaer, S. De Troch (IMEC)
"The HOP system"
G. Gopalakrishnan, Univ. of Calgary
"LAMBDA"
R. Harris, M. Fourman, Abstract Hardware Ltd.
"The Boyer-Moore Theorem Prover"
W. Hunt, B. Brock, Computational Logic Inc.
"T.U. Eindhoven Verification tools"
G. Janssen, G. de Jong, Tech. Univ. Eindhoven
"RLEXT: manual optimization program"
D. Knapp, Univ. of Illinois
"HIFI"
A. de Lange, Technical Univ. Delft
"The formal verifier PRIAM"
J-C Madre, Bull
"Functional extraction of hierarchical sequential systems."
F. Martinolle, B. Sousal, J.-C. Geffroy, Inst. Nat. Sciences Appliquées.
"Maple"
F Mavaddat, Univ. of Waterloo
"Fast Tautology Checking Using Shared Binary Decision Diagram"
S. Minato, N. Ishiura, S. Yajima, Kyoto Univ.
"The Edinburgh Concurrency Workbench"
F. Moller, University of Edinburgh
"Formal proof of "Min-max" benchmark from CASCADE in Boyer-Moore"
L Pierre, Univ de Provence
"The NODEN hardware verification suite."
C. Pygott, RSRE
"Non-standard interpretation of HDL's"
S. Singh, University of Glasgow.
"CLIO"
M.K. Srivas, Odyssey Research Associates
"Verification of VLSI Circuits using LP"
J. Staunstrup, Technical Univ. of Denmark.

"Applications of Finite State Modelling and Analysis in Asynchronous/Synchronous Circuit Design"
P.A. Subrahmanyam, AT&T Bell Labs, Holmdel

"A New Algorithm for Transistor Netlist Comparison"
E.Vanden Meersch, CPqD Telebras, Campinas

"PRESAGE"
V.Van Dongen, M.Petit, Philips Res Labs, Brussels

"Tautology Checker for VLSI Applications that Simplifies More and Backtracks Less"
F. Vlach, Univ. of North Texas

Table of Contents.

Chapter 1: MOS Circuit Level Verification.

Chapter 2: Efficient Tautology Checking Algorithms.

Chapter 3: Verification of Sequential Machines.

Chapter 4: Functionality Extraction, Comparison and Testing.

Register Transfer Level Verification.

Chapter 6: Boyer-Moore Theorem Prover Based Verification.

Chapter 7: Hardware Verification using HOL.

Chapter 1

MOS Circuit Level Verification.

FORMAL VLSI CORRECTNESS VERIFICATION
VLSI Design Methods, II
L.J.M. Claesen (Editor)
Elsevier Science Publishers B.V. (North-Holland)
© IFIP, 1990

BEAVER: A BEHAVIORAL FORMAL VERIFIER FOR VLSI DESIGN

Seung Ho Hwang
Schlumberger Technologies
1601 Technology Drive
San Jose, CA 95110-1397
U.S.A.

A. Richard Newton
Department of Electrical Engineering and Computer Science
University of California
Berkeley, CA 94720
U.S.A.

The formal verifier, *BEAVER*, developed in this work, checks the equivalence of two behavioral descriptions. The approach is based on theorem proving methods. Because verification is performed by a formal technique, complete verification can be achieved without exhaustive simulation. Behavior is specified in a hardware description language that deals with timing and functionality in one paradigm using functional (denotational) semantics. Type definition mechanisms and macros are provided, along with recursive definitions. The behavioral verification system automatically handles type definitions and exploits hierarchy. Hierarchy is exploited when checking functional equivalence by using techniques such as inductive verification of recursive descriptions. Hierarchical timing verification is also supported by the abstraction of timing information by constraint propagation. During the abstraction of timing information, the availability of functional relations between signals eliminates the static-insensitizable-path problem.

1. INTRODUCTION

The ultimate goal of computer-aided design (CAD) of integrated circuits(IC's) is to build systems which can generate automatically designs of entire circuits from the user-supplied requirements. However, the achievement of this goal is not foreseeable in the near future. Current approaches involve human intervention, and design verification continues to be an important problem.

Traditionally, simulation at various levels of description has been used for the verification of hardware design. In order to achieve a complete verification using this approach, exhaustive simulation must be performed. Unfortunately, excluding very simple designs, exhaustive simulation is nearly impossible. To overcome this limitation, formal verification techniques have been proposed [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15]. However, in order to apply these techniques to real design problems, more research work is needed.

In this paper the practicality of the hardware design verification is addressed in an effort to narrow the gap between the theory and its application to real problems.

To address the complexity of a VLSI design, the concept of hierarchical design has been widely accepted. When a design is performed in a hierarchical environment, the verification of a large system can be split into smaller and simpler problems. This "divide-and-conquer" approach provides a practical approach to solving the complex verification problem. The increasing importance of the logical structure in VLSI design [16, 17], demands methodologies and tools to support hierarchical decomposition at high levels.

In BEAVER, not only the functional behavior but also the timing behavior is verified. Most timing verifiers deal with flattened-down descriptions of a design at a specific level, usually in switch-level or gate-level [18, 19, 20]. However, with hierarchical descriptions it is more desirable to be able to handle the timing information in a hierarchical manner. The abstraction of timing behavior, as well as functionality, is important. Also, as the timing verification is performed with the known functional relations of signals, the static-insensitizable-path problem, which has been an important problem in timing verification, can be eliminated.

The organization of the paper is as follows. In Section 2, the overview of the verification system is presented. The behavioral description language used in BEAVER is introduced in Section 3. The timing verification part of the behavioral verifier is presented in Section 4. Section 5 deals with the functional verification aspect of the behavioral verifier. Conclusions and future research work are included in Section 6.