VLSI SPECIFICATION, VERIFICATION AND SYNTHESIS

THE KLUWER INTERNATIONAL SERIES IN ENGINEERING AND COMPUTER SCIENCE

VLSI, COMPUTER ARCHITECTURE AND DIGITAL SIGNAL PROCESSING

Consulting Editor

Jonathan Allen

Other books in the series:

Introduction to VLSI Silicon Devices: Physics, Technology and Characterization,
B. El-Kareh and R. J. Bombard.
ISBN 0-89838-210-6.
Latchup in CMOS Technology: The Problem and Its Cure,
R. R. Troutman.
ISBN 0-89838-215-7.
Digital CMOS Circuit Design,
M. Annaratone.
ISBN 0-89838-224-6.
The Bounding Aproach to VLSI Circuit Simulation,
C. A. Zukowski.
ISBN 0-89838-176-2.
Multi-Level Simulation for VLSI Design,
D. D. Hill and D. R. Coelho.
ISBN 0-89838-184-3.
Relaxation Techniques for the Simulation of VLSI Circuits,
J. White and A. Sangiovanni-Vincentelli.
ISBN 0-89838-186-X.
VLSI CAD Tools and Applications,
Wolfgang Fichtner and Martin Morf, Editors.
ISBN 0-89838-193-2.
A VLSI Architecture for Concurrent Data Structures,
W. J. Dally.
ISBN 0-89838-235-1.
Yield Simulation for Integrated Circuits,
D. M. H. Walker.
ISBN 0-89838-244-0.

VLSI SPECIFICATION, VERIFICATION AND SYNTHESIS

edited by

Graham Birtwistle
University of Calgary

and

P.A. Subrahmanyam
AT&T Bell Laboratories

KLUWER ACADEMIC PUBLISHERS
Boston/Dordrecht/Lancaster

Distributors for North America:
Kluwer Academic Publishers
101 Philip Drive
Assinippi Park
Norwell, Massachusetts 02061, USA

Distributors for the UK and Ireland:
Kluwer Academic Publishers
MTP Press Limited
Falcon House, Queen Square
Lancaster LA1 1RN, UNITED KINGDOM

Distributors for all other countries:
Kluwer Academic Publishers Group
Distribution Centre
Post Office Box 322
3300 AH Dordrecht, THE NETHERLANDS

Library of Congress Cataloging-in-Publication Data

VLSI specification, verification, and synthesis / by Graham Birtwistle and P.A. Subrahmanyam [editors].
p. cm.—(The Kluwer international series in engineering and computer science ; SECS 35)
A collection of papers presented at a workshop held in Calgary, Canada, Jan. 12–16, 1987.
ISBN-13: 978-1-4612-9197-8 e-ISBN-13: 978-1-4613-2007-4
DOI: 10.1007/978-1-4613-2007-4
1. Integrated circuits—Very large scale integration—Design and construction. I. Birtwistle, G. M. (Graham M.) II. Subrahmanyam, P. A. III. Series.
TK7874.V564 1988
621.395—dc19

Contents

Preface

VLSI Specification, Verification and Synthesis
Proceedings of a workshop
held in Calgary from 12-16 January 1987.

The collection of papers in this book represents some of the discussions and presentations at a workshop on hardware verification held in Calgary, January 12-16 1987. The thrust of the workshop was to give the floor to a few leading researchers involved in the use of formal approaches to VLSI design, and provide them ample time to develop not only their latest ideas but also the evolution of these ideas.

In contrast to simulation, where the objective is to assist in detecting errors in system behavior in the case of some selected inputs, the intent of hardware verification is to formally prove that a chip design meets a specification of its intended behavior (for all acceptable inputs). There are several important applications where formal verification of designs may be argued to be cost-effective. Examples include hardware components used in "safety critical" applications such as flight control, industrial plants, and medical life-support systems (such as pacemakers). The problems are of such magnitude in certain defense applications that the UK Ministry of Defense feels it cannot rely on commercial chips and has embarked on a program of producing formally verified chips to its own specification. Hospital, civil aviation, and transport boards in the UK will also use these chips. A second application domain for verification is afforded by industry where specific chips may be used in high volume or be remotely placed. The cost of a flawed telecommunications chip design might mean a prohibitive replacement program. Simply because of their locations, sensor chips installed on pipelines and surveillance chips in polar regions would be tremendously expensive to replace should their designs be faulty. A third application area is product redesign. Technology advances mean that chips have to be reworked into a new technology every two or three years, or even less. If a design has a verified design development tree, redesign to account for changes in technology will typically involve a replacement of the lower subtrees. There need be no change to the overall chip specification if the behaviors of the replacement designs conform to the specification of their plug-in slot in the new tree. In this case, the new versions of the same part can be inserted into existing systems with a guarantee that they will not introduce new bugs.

The major themes of the workshop are presented here in four sections. First, the state of the art in hardware verification and specification is covered with two papers on the VIPER chip and its proof. VIPER is the first production microprocessor chip to be formally verified and implemented in silicon. The second section presents Mike Gordon's

Higher Order Logic System (HOL) which has been used for several substantial verification efforts. The papers explain how to construct proofs in HOL and give several examples of HOL in use as a hardware description language describing circuits ranging is size from leaf cells through sub-systems all the way through to a complete (but small) microprocessor. The third section discusses some ideas for automated CAD systems using formal specifications. The final section covers transistor level modelling, a proof system for a development of Mossim, the verification of a dynamic CMOS circuit design style, and the use of abstraction mechanisms in verification.

The VIPER chip and its proof. The first paper, by John Cullyer, describes the design and development of the VIPER microprocessor. In order to satisfy certification authorities of the correctness of the processor's implementation, semi-formal mathematical methods were used, both to specify the overall behavior of the processor and to prove that two different gate level realizations conform to this top level specification. The second paper on VIPER by Avra Cohn (not read at the workshop) complements Cullyer's overall description and design insights. It details formal mechanization of the first two levels of the semi-formal proof developed by RSRE (The Royal Systems and Radar Establishment in UK). The mechanical verification was a formidable task, which revealed several small flaws with the original hand proof. Three of the flaws revealed were of a more serious nature: a phase error in the fetch cycle, and some incomplete checks for illegal instructions due to unforeseen conditions. Cohn's work would seem to vindicate completely formal methods.

HOL. VIPER demonstrates that existing design and verification techniques can be applied to complex synchronous circuits in a practical manner. Future automated verification tools need to be interfaced to industrial VLSI systems and transform specifications to layout without human intervention. The second section concentrates upon Mike Gordon's HOL (a mechanization of Higher Order Logic). Many of the largest proofs completed to date have been constructed using either Mike's LCF-LSM system or its successor HOL. HOL has already shown (by construction) that it can handle circuits, sub-systems and complete architectures. Thus one notation can span the whole VLSI spectrum. What is lacking at the moment is the ability to incorporate electrical properties into HOL definitions; constraints fit are readily incorporated into the HOL pattern. Gordon's paper gives an introduction to the properties of the HOL language, its proof support apparatus, and small examples of an interactive proof in HOL. Jeff Joyce discusses his reworking in HOL of Gordon's original LCF-LSM proof of a toy microprocessor.

VLSI CAD environments. The Synapse environment is intended to support the development of provably correct designs, proceeding from high level behavioral specifications and optional performance criteria. Its features include various flavors of expert system support, as well as support for formal manipulations; ways of incorporating order of magnitude constraints along dimensions such as area and response time; and a leaf cell synthesizer that has generated novel CMOS circuits. An important issue in the context of such high level design tools is that of *system timing*, which deals with the relative sequencing of subcomputations, the detailed behavior of signal voltages over time, and overall system performance. The design of a VLSI system typically involves many decisions relating to several levels of timing detail. Examples include choices relating to timing disciplines, architectural and circuit design paradigms, the number of clock phases, the number of amplification stages, the sizes of specific transistors, and the temporal behavior demanded of specific input signals (such as stability criteria they must obey). Subrahmanyam's paper introduces a framework for dealing with system timing issues in the context of very high level silicon compilers. The paradigm considered allows the details of system timing to be *gradually* introduced as a design progresses. During the early stages of a design, no timing details need be explicit, and the only temporal constraints arise due to functionality, causality and stability criteria. As a design evolves, and decisions relating to resource allocation, computation schedules, timing and clocking disciplines are made, the temporal constraints on signals evolve correspondingly. If the external environment in which a system resides imposes any *a priori* temporal constraints, such constraints can be explicitly included in the initial specification, and accounted for in the synthesis process. The framework supports synchronous and asynchronous (self-timed) disciplines, multiphase-clocks, as well as techniques that bear on optimizations of performance metrics such as power and area.

The paper by Musser *et al* outlines an approach to verification based on the formalism of abstract data types, and as implemented in the Affirm system. The paper by Narendran *et al* describes work on the Interactive VHDL workstation (IVW) project that uses the Rewrite Rule Laboratory (RRL) theorem prover. The main goals of this project are to furnish the user with textual and graphical capabilities to enter and modify his behavioral and structural specifications, and tools to relate these specifications to formulas for input to the Rewrite Rule Laboratory theorem prover. The final paper in this section, by George Milne, sketches a technique where specifications, designs and contextual information are all described in a common language. Contextual knowledge is captured as just another expression in the language and may be used to simplify the representation of a design in a rigorous

manner.

Modelling and abstraction. Tom Melham addresses abstraction issues in specification. Abstract specifications of design components are used to derive more compact descriptions of behavior. By doing this at each level of a hierarchically structured design, the size and complexity of a large proof can be controlled. Thus, abstraction mechanisms complement structural hierarchy in handling proofs of large systems. Glynn Winskel discusses several models of MOS circuits and points out some of their shortcomings. Bryant's model, used in Mossim II, tackles such issues in reasonable generality and has been used as the basis of several MOS switch-level simulators; however, this model is not compositional. Winskel presents a compositional model for the behavior of MOS circuits when the input is steady, and shows how this leads to a formal logic. He also indicates the difficulties in providing a full and accurate treatment for circuits with changing inputs. Inder Dhingra formalizes some rules of thumb for popular CMOS design styles, and uses them to analyze the rules of the NORA design style. In this design style, there are two complementary clock lines, and p- and n-type gates. The design rules govern how the gates may be connected, what clock lines they are driven by, and if the output is to be guaranteed. In order to make the design style synchronous, a CMOS latch is used as a dynamic register. This further complicates the rules but gives rise to a design style that generates smaller and faster circuits as compared to standard CMOS. Dhingra goes on to prove that the NORA design style can fail for large circuits, and develops CLIC, a refinement of NORA using a two phase non-overlapping clocking scheme that is guaranteed. Dhingra also gives a formal motivation for the design style using a simple transistor model with charge storage capability. Steve Johnson discusses work-in-progress on the automation of digital-design synthesis from functional specifications via transformations. He describes work concerned with systematically obtaining correct physical implementations from iterative specifications, and with building aids to facilitate the process. The motivation is to develop a practical methodology with an algebraic flavor. Christian Berthet presents a methodology for comparing switch-level circuits with their high-level specifications wherein circuits, user behavior and input constraints are modelled as asynchronous machines. The model is based on characteristic functions. A Boolean algebra of asynchronous machines is defined. Machine composition and internal variable abstraction are shown to correspond respectively to the product and sum operations of the algebra. Internal variables can be abstracted under the presence of a domain constraint, provided that the I/O behavior is preserved. The verification of a speed-independent fair arbiter is presented to exemplify the techniques.

Acknowledgements. The workshop was funded by the Natural Sciences and Engineering Research Council of Canada through an Operating Grant, by the University of Calgary, and by the Department of Computer Science at the University of Calgary. The Alberta Microelectronics Center kindly furnished the location and kept us going with coffee throughout the week. The workshop organizers would like to thank those who made the job easy: the speakers who provided excellent written material beforehand, and the participants for many lively discussions which never got (completely) out of hand.

Graham Birtwistle, *University of Calgary.*
P.A.Subrahmanyam, *AT&T Bell Laboratories.*