# Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

408

M. Leeser G. Brown (Eds.)

# Hardware Specification, Verification and Synthesis: Mathematical Aspects

Mathematical Sciences Institute Workshop
Cornell University, Ithaca, New York, USA
July 5–7, 1989
Proceedings

Springer-Verlag
Berlin Heidelberg New York London Paris Tokyo Hong Kong

**Editors**

Miriam Leeser
Geoffrey Brown
School of Electrical Engineering, Cornell University
Ithaca, New York 14853-5401, USA

CR Subject Classification (1987): B.5.2, B.6.3, B.7.2, F.3.1, F.4.1, I.2.3

ISBN 0-387-97226-9 Springer-Verlag New York Berlin Heidelberg
ISBN 3-540-97226-9 Springer-Verlag Berlin Heidelberg New York


Printed in Germany

Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
2145/3140-543210 – Printed on acid-free paper

# Introduction

This proceedings contains the papers presented at a workshop held at Cornell University in Ithaca, New York, during July 5-7, 1989. The workshop was sponsored by the Army Research Office through the Mathematical Sciences Institute.

The goal of the workshop was to present current research into formal methods for hardware design. Because of the complexity of VLSI circuits, assuring design validity before circuits are manufactured is imperative. The goal of research in this area is to develop methods of improving the design process and the quality of the resulting designs. The analytic tool of this research is logic; the fundamental problems are to develop ways of using logic to specify systems, model hardware, and verify designs; and to develop tools (for example, theorem provers) that simplify the application of logic to hardware specification and synthesis.

The workshop was attended by over 70 researchers from North America and Europe and papers were presented by 20 invited lecturers. In developing the workshop program, we tried to include representatives from a diverse set of hardware verification projects and geographical regions. We believe that this goal was achieved with one exception – continental Europe is not represented though there are several important projects that would have been appropriate. Funding constraints forced us to focus most of our program on research being performed in the United States. As a result, the workshop provided a forum for US researchers in formal methods for hardware to present their work in the United States. Previously they have had to travel to Europe or Canada to present their results.

The major trend apparent at the workshop is that researchers are rapidly moving away from *post hoc* proof techniques which have received considerable criticism for their great expense. A number of papers were presented that dealt with problems of synthesizing correct circuits and of designing with the goal of verification. In addition, researchers are beginning to deal with the difficult theoretical issues of reasoning about concurrent systems and asynchronous systems. The workshop also saw the introduction of constructive type theory and category theory into the hardware verification community thus providing new logical tools.

The area of formal methods encompasses three major issues: specification, verification, and synthesis. Each of these was addressed at the workshop.

There is no consensus on the best type of specification language to use for formal hardware tools. This is primarily due to the tradeoffs between expressiveness and ease of automated proof. Two types of specification languages have found the widest acceptance – functional programming languages and higher order logics – with higher order logic being more expressive, and consequently more difficult to mechanize. Papers based upon the higher order logic (HOL) approach were presented by Brian Graham, Paul Loewenstein, Shiu-kai Chin, and Jeffrey Joyce. The functional programming view was supported by papers presented by Steven Johnson, Warren Hunt, and M. K. Srivas. Even more expressive than HOL is constructive type theory and, at the workshop, some of the first results by researchers using this form of logic were presented. These included papers presented by Miriam Leeser,

Peter Del Vecchio, and Keith Hanna. In addition a paper on category theory was presented by Mary Sheeran.

Several speakers presented results on the verification of actual systems. While *post hoc* proof is extremely time consuming, it serves the useful function of driving the development of specification languages and of developing our ability to reason about complex systems. The papers presented on verification considered quite complex systems such as processors (Brian Graham and Graham Birtwistle, M.K. Srivas) and vertically verified systems consisting of a compiler and an underlying processor (Joyce).

The issues of synthesis of correct circuits and design for verification were discussed by Chris Lengauer, George Milne, Miriam Leeser, Raul Camposano and Steve Johnson.

For many years asynchronous design has not been widely used, and the circuits designed have tended to be small. These circuits were simply too hard to design, and the available tools were inadequate. Recently, the application of formal design techniques has led to a revival of asynchronous circuits by making their design more tractable. Papers supporting this revival were presented by P.A. Subrahmanyam, David Dill, and Alain Martin.

Formal methods have been slow to find their way into standard engineering practice; however, it appears that this will soon change. Randy Bryant presented a paper demonstrating the use of formal techniques to speed up traditional hardware simulation tools.

We would like to thank Bob Constable for presenting the welcome address and the following people for chairing sessions: Bob Constable, Beth Levy, Jo Ebergen, Mike Fourman, Jim Caldwell, and Geraint Jones.

Miriam E. Leeser
Geoffrey M. Brown



## Table of Contents