ABSTRACTION REFINEMENT FOR LARGE SCALE MODEL CHECKING

SERIES ON INTEGRATED CIRCUITS AND SYSTEMS

Anantha Chandrakasan, Editor
Massachusetts Institute of Technology
Cambridge, Massachusetts, USA

Published books in the series:

A Practical Guide for SystemVerilog Assertions
Srikanth Vijayaraghavan and Meyyappan Ramanathan
2005, ISBN 0-387-26049-8

Statistical Analysis and Optimization for VLSI: Timing and Power
Ashish Srivastava, Dennis Sylvester and David Blaauw
2005, ISBN 0-387-25738-1

Leakage in Nanometer CMOS Technologies
Siva G. Narendra and Anantha Chandrakasan
2005, ISBN 0-387-25737-3

Thermal and Power Management of Integrated Circuits
Arman Vassighi and Manoj Sachdev
2005, ISBN 0-398-25762-4

High Performance Energy Efficient Microprocessor Design
Vojin Oklobdzija and Ram Krishnamurthy (Eds.)
2006, ISBN 0-387-28594-6

ABSTRACTION REFINEMENT FOR LARGE SCALE MODEL CHECKING

CHAO WANG
NEC Laboratories America
Princeton, New Jersey

GARY D. HACHTEL
University of Colorado
Boulder, Colorado

FABIO SOMENZI
University of Colorado
Boulder, Colorado

Chao Wang
NEC Laboratories America
4 Independence Way, Suite 200
Princeton, New Jersey 08540
U.S.A.

Gary D. Hachtel
University of Colorado
Department of Electrical/Computer Engineering
Campus Box 425
Boulder, Colorado 80309
U.S.A.

Fabio Somenzi
University of Colorado
Department of Electrical/Computer Engineering
Campus Box 425
Boulder, Colorado 80309
U.S.A

Abstraction Refinement for Large Scale Model Checking

Library of Congress Control Number: 2006926215

ISBN-10: 0-387-34155-2
ISBN-13: 9780387341552
ISBN-10: 0-387-34600-7 (e-book)
ISBN-13: 9780387346007 (e-book)

Printed on acid-free paper.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1

springer.com

Contents

List of Figures

List of Tables

Preface

This book summarizes our research work conducted in the University of Colorado at Boulder from 2000 to 2004 while the first author was pursuing his Ph.D. degree in the Department of Electrical and Computer Engineering. Our research addresses the problem of applying automatic abstraction refinement to the model checking of large scale digital systems.

Model checking is a formal method for proving that a finite state transition system satisfies a user-defined specification. The primary obstacle to its widespread application is the capacity problem: State-of-the-art model checkers cannot directly handle most industrial-scale designs. Abstraction refinement—an iterative process of synthesizing a simplified model to help verify the original model—is a promising solution to the capacity problem. In this book, several fully automatic abstraction refinement techniques are proposed to efficiently reach or come close to the simplest abstraction.

First, a fine-grain abstraction approach is proposed to keep the abstraction granularity small. With the advantage of including only the relevant information, the fine-grain abstraction is proved to be indispensable in verifying systems with complex combinational logic. A scalable game-based refinement algorithm called GRAB is proposed to identify the refinement variables based on the systematic analysis of all the shortest counterexamples. Compared to methods in which each refinement is guided by a single counterexample, this algorithm often produces a smaller abstract model that can prove or refute the same property.

Second, a compositional SCC analysis algorithm called DNC is proposed in the context of LTL model checking to quickly identify unimportant parts of the state space in previous abstractions and prune them away before verification is applied to the next abstraction level. With a speed-up of up to two orders of magnitude over standard symbolic fair

cycle detection algorithms, DnC demonstrates the importance of reusing information learned from previous abstraction levels to help verification at the current level.

Finally, BDD based symbolic image computation and Boolean satisfiability check are revisited in the context of abstraction refinement. We propose two new algorithms in order to improve the computational efficiency of BDD based symbolic fixpoint computation and SAT based bounded model checking, by applying the idea of abstraction and successive refinements inside the two basic decision procedures.

Analytical and experimental studies demonstrate that the fully automatic abstraction refinement techniques proposed in this book are the key to applying model checking to large systems. The suite of fully automatic abstraction refinement algorithms has demonstrated significant practical importance. Some of these BDD and SAT based algorithms have been adopted by various commercial/in-house verification tools in industry.

The Ph.D. dissertation upon which this book is based won the 2003-2004 ACM outstanding Ph.D. dissertation award in electronic design automation. This ACM award, established by ACM SIGDA, is given each year to an outstanding Ph.D. dissertation that makes the most substantial contribution to the theory and/or application in the field of electronic design automation.

CHAO WANG, GARY D. HACHTEL, FABIO SOMENZI

Acknowledgments

We are grateful to our editor Carl Harris and his colleagues at Springer for their help on making the book idea into a reality. This book is a revision of my dissertation for the Ph.D. degree in Electrical Engineering in the University of Colorado at Boulder. Below is the acknowledgment from the original version of the dissertation.

I want to thank my research advisors Professor Gary D. Hachtel and Professor Fabio Somenzi for giving me the opportunity to explore the area of formal verification. This dissertation could not have been possible without their guidance and financial support in the past four years. I also want to thank Dr. Robert Brayton, Dr. Harold Gabow, Dr. Aarti Gupta, and Dr. Sunil Khatri for kindly serving on my Ph.D. thesis committee.

This research builds upon the prior work of many people. I would like to thank Dr. Roderick Bloem and Dr. Kavita Ravi for their helpful discussions during the early years of my study. My collaboration with them has been very fruitful [WBH+01, WH02]. I would also like to thank Dr. Pei-Hsin Ho, Dr. Pranav Ashar, Dr. Malay Ganai, and Dr. Zijiang Yang. My summer internships at Synopsys and NEC Labs not only allowed me to conduct cutting edge research [GGW+03b, GGW+03a], but also gave me the opportunity to attack real-world hardware verification problems from industry.

Many thanks are due to present members of our research group. Graduate study is largely an individual effort in fighting anxieties; there can be a lot of days when the research simply seems to go nowhere. I am lucky to have a group of fellow students in the VLSI/CAD lab who believe in interaction and cooperation. Their help was invaluable. I want to thank Bing Li and HoonSang Jin for their productive collaboration [WHS03, WJHS04]. It is also a lot of fun working with Moham-

mod Awedh, Mitra Purdandare, David Ward, Nikhil Jayahumar, Nikhil Saluja, and Chunjie Duan.

Finally, my thanks to my parents and my wife Hui Yang for their love and support.

Chao Wang
Boulder, Colorado