

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



Springer

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.

© 2006 Springer Science+Business Media, LLC

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1

springer.com

Contents

List of Figures	vii
List of Tables	ix
Preface	xi
Acknowledgments	xiii
1. INTRODUCTION	1
1.1 Background	3
1.2 Our Contributions	5
1.3 Organization of This Book	9
2. SYMBOLIC MODEL CHECKING	11
2.1 Finite State Model	12
2.2 Temporal Logic Property	15
2.3 Generalized Büchi Automaton	20
2.4 BDD-based Model Checking	27
2.5 SAT and Bounded Model Checking	33
2.6 Abstraction Refinement Framework	38
3. ABSTRACTION	41
3.1 Introduction	42
3.2 Fine-Grain Abstraction	43
3.3 Abstract Counterexamples	48
3.4 Further Discussion	52
4. REFINEMENT	55
4.1 Generational Refinement	56
4.2 Refinement Variable Selection	62

4.3	Keeping Refinement Set Small	67
4.4	Applying Sequential Don't Cares	70
4.5	Implementation and Experiments	72
4.6	Further Discussion	77
5.	COMPOSITIONAL SCC ANALYSIS	85
5.1	Language Emptiness	86
5.2	SCC Partition Refinement	88
5.3	The D'n'C Algorithm	91
5.4	The Composition Policies	97
6.	DISJUNCTIVE DECOMPOSITION	101
6.1	Adaptive Popcorn-line Policy	101
6.2	Disjunctive Decomposition Theorem	103
6.3	Guided Search for Fair Cycles	105
6.4	Implementation and Experiments	109
6.5	Further Discussion	114
7.	FAR SIDE IMAGE COMPUTATION	121
7.1	Symbolic Image Computation	121
7.2	The Far Side Image Algorithm	124
7.3	Experiments	127
7.4	Discussion of Hypothesis	130
8.	REFINING SAT DECISION ORDERING	137
8.1	Unsatisfiability Proof as Abstraction	137
8.2	Refining The Decision Ordering	142
8.3	Experimental Analysis	146
8.4	Further Discussion	151
9.	CONCLUSIONS	153
9.1	Summary of Results	153
9.2	Future Directions	155
	References	157
	Index	177

List of Figures

2.1	An example of the Kripke structure.	13
2.2	A sequential circuit example.	14
2.3	A Kripke structure and its computation tree.	19
2.4	The relationship among LTL, CTL, and CTL*.	19
2.5	An LTL model checking example.	23
2.6	Two terminal generalized Büchi automata.	30
2.7	A bounded model checking instance.	35
2.8	The DLL Boolean SAT procedure.	37
2.9	The abstraction refinement framework.	39
3.1	Illustration of fine-grain abstraction.	46
3.2	Ariadne's bundle of synchronous onion rings.	50
3.3	Multi-thread concretization test.	52
3.4	Translating a BDD into a combinational circuit.	53
4.1	An example for abstraction refinement.	56
4.2	The generational refinement process.	58
4.3	The effect of generational refinement, with refinement minimization.	59
4.4	The GRAB abstraction refinement algorithm.	61
4.5	Illustration of the winning positions.	64
4.6	An example for state splitting.	66
4.7	Another example for state splitting.	67
4.8	Sequential Don't Cares from remaining submodules.	71
4.9	Comparing the abstraction efficiency of different refinement algorithms.	75

4.10	The CPU time distribution among the different phases of abstraction refinement.	83
5.1	Parallel composition of automata and its impact on SCCs.	91
5.2	The generic SCC analysis algorithm D’N’C.	92
5.3	An example of using don’t cares in the computation of SCCs.	95
5.4	Another example of using don’t cares in the computation of SCCs.	96
5.5	Lattice of approximations.	98
5.6	An SCC partition refinement tree.	100
6.1	Guided search of fair cycles and sharp image.	108
7.1	The Far Side image computation algorithm.	125
7.2	Minimizing the transition relation.	126
7.3	s5378opt: The upper part is the BDD size of the intermediate products at different steps during the reachability analysis; the lower part is the total number of live BDD nodes, including BDDs representing the accumulated reachable states.	132
7.4	The BDD size reduction of the transition relation, in terms of the ratio of the BDD size of minimized transition relation to the original BDD size.	134
8.1	Illustration of the resolution graph.	139
8.2	From unsatisfiable cores to abstractions.	140
8.3	Previous abstractions to help solving the current BMC instance.	141
8.4	Refining the SAT decision order in bounded model checking.	143
8.5	Scatter plots: plain BMC vs. BMC with the refined ordering.	148
8.6	Reduction of the size of decision trees.	149
8.7	Reduction of the number of conflicts and implications.	150

List of Tables

4.1	Comparing invariant checking algorithms.	80
4.2	Correlation between the final proofs of GRAB and CA.	81
4.3	Comparing GRAB, +FINEGRAIN, and +ARDC.	82
6.1	Comparing Emerson-Lei and D'n'C. With RDC's.	116
6.2	Comparing EL, D'n'C, and D'n'C#. With RDC's.	117
6.3	Comparing EL, D'n'C, and D'n'C#. With ARDC's.	118
6.4	Comparing EL, D'n'C, and D'n'C#. With ARDC's.	119
7.1	Comparing FAR SIDEIMG and MLP with dynamic variable reordering.	129
7.2	Comparing FAR SIDEIMG and MLP with fixed variable ordering.	131
8.1	Comparing BMC with and without refining the SAT decision order.	147

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-

xiv

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