ABSTRACT

DUVARNEY, DANIEL C. Abstraction-Based Generation of Finite State Models
from C Programs. (Under the direction of Associate Professor S. Purushothaman Iyer).

Model checking is a major advancement in the quest for practical automatic ver-
ification methods for computer systems, and has been effectively used to discover flaws in
real-world hardware systems. Unfortunately, applying model-checking techniques to soft-
ware systems has proved to be more difficult, due to the large number of states and irregular
transitions of such systems. One promising method for generating reasonably-sized models
from programs is the use of *data abstraction*, in which the program data is mapped from a
large set of possible values to a much smaller set of abstract values. This thesis develops
a method which, given a program in the C language and an abstraction mapping, allows
the automatic construction of an abstract labeled transition system (LTS), which is much
smaller than the concrete LTS (the LTS which would be generated without the benefit of
abstraction). The method is shown to be *sound* in the sense that if a program is well-
behaved in its use of pointers, then any linear temporal logic formula which holds true for
the corresponding abstract LTS will also hold true for the concrete LTS. Furthermore, if
a design exists in the form of a transition system, then the abstract LTS can be checked
against the design for bisimilarity. Bisimilarity ensures that the program is a faithful im-
plementation of the design. A suite of software tools has been implemented based upon
the theory. These tools interface with the Concurrency Workbench, a model checking sys-
tem. A case study is presented which shows the practicality of this technique for verifying
real-world C programs.

Abstraction-Based Generation of Finite State Models
from C Programs

by

Daniel C. DuVarney

A dissertation submitted to the Graduate Faculty of
North Carolina State University
in partial satisfaction of the
requirements for the Degree of
Doctor of Philosophy

Department of Computer Science

Raleigh

2002

Approved By:

_____	_____
Dr. K. C. Tai	Dr. John W. Baugh, Jr.
_____	_____
Dr. S. Purushothaman Iyer	Dr. W. Rance Cleaveland II
Chair of Advisory Committee	

Your dedication goes here . . .

Biography

Put your bio here ...

Acknowledgements

Acknowlegements go here...

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Summary and overview of thesis

Chapter 2

The Problem

A statement of the problem

Chapter 3

Related Work

Previous attempts to solve the problem

Chapter 4

Theory

A theoretical solution

Chapter 5

Implementation

An implementation based on the theory

Chapter 6

Case study

Experimental Results [**?**]

Chapter 7

Conclusion

Why your work is better and future work [**?**]