AIN SHAMS UNIVERSITY

FACULTY OF ENGINEERING

Computer and Systems Engineering

Embedded Software Coverage Analysis using Model Checking

A Thesis submitted in partial fulfilment of the requirements of the degree of

Master of Science in Electrical Engineering

Computer and Systems Engineering

by

Nahla Mohamed Mohamed Saleh

Master of Science in Electrical Engineering

Computer and Systems Engineering

Faculty of Engineering, Ain Shams University, 2017

Supervised By

Prof. Dr. Ashraf Mohamed El-Farghally Salem

Prof. Dr. Ayman Mohamed Mohamed Hassan Wahba

Dr. Mona Mohamed Hassan Safar

Cairo - (2017)

AIN SHAMS UNIVERSITY

FACULTY OF ENGINEERING

Computer and Systems Engineering

Embedded Software Coverage Analysis using Model Checking

by

Nahla Mohamed Mohamed Saleh

Master of Science in Electrical Engineering

Computer and Systems Engineering

Faculty of Engineering, Ain Shams University, 2016

Examiners' Committee

Name and Affiliation	**Signature**
Prof. Dr. Ashraf Mohamed El-Farghally Salem Computer Engineering and Systems Faculty of Engineering, University	…….
Prof. Dr. Ayman Mohamed Mohamed Hassan Wahba Computer Engineering and Systems Faculty of Engineering, University	…….
Dr. Mona Mohamed Hassan Safar Computer Engineering and Systems Faculty of Engineering, University	…….

Date:25 April 2017

Statement

This thesis is submitted as a partial fulfilment of Master of Science in Electrical Engineering, Faculty of Engineering, Ain shams University.

The author carried out the work included in this thesis, and no part of it has been submitted for a degree or a qualification at any other scientific entity.

Student name

Nahla Mohamed Mohamed Saleh

Signature

……...…….

Date:25 April 2017

Researcher Data

Name: Nahla Mohamed Mohamed Saleh

Date of birth: 06/03/1984

Place of birth: Cairo, Egypt

Last academic degree: Bachelor of Science

Field of specialization: Computer and Science

University issued the degree: Ain Shams University

Date of issued degree: 2006

Current job: Senior Quality Assurance/Test Engineer

Faculty of Engineering

Computer and Systems Engineering

Abstract

Embedded Software Coverage Analysis using Model Checking

Nahla Mohamed Mohamed Saleh

Embedded systems, like smart phones, laptops, servers, etc. are intruding the market with high acceleration. Many studies have proven that up to 70% of the development cycle is spent in the verification. A significant stage in the development cycle of the embedded system is the validation of the hardware models. The goal of this work is to shorten the hardware validation stage time. Our approach is to get the related test cases ready before the hardware exists. It mainly depends on deploying a formal methodology on the virtual hardware model for an Automatic Test Pattern Generation. The first phase in our approach involves the creation of harness based on constraints extracted from the specification. The main goal of the harness is to tackle the challenges of deploying formal methodology to generate high functional coverage test cases. The second phase involves the replay of the test cases to provide an early evaluation of the test coverage before the RTL exists. For this purpose, we developed a semi-automated methodology to compute and report the test coverage. Therefore, when the hardware is ready, these test cases can be directly deployed for coverage verification. We have applied our approach on a QEMU Direct Memory Access controller to evaluate the test coverage for the generated test suite. Furthermore, we have applied the test suite on the corresponding Register Transfer Level model. The results demonstrate that our test suite is able to meet the coverage goal on the register transfer level using Universal Verification Methodology test environment.

Key words: Formal methodology; Virtual Hardware Model; Functional coverage verification; Automatic Test Pattern Generation; Universal Verification Methodology test environment

Acknowledgment

This thesis could not have been accomplished without the generous help and support from many professors, friends and my family. I would like to express my sincere gratitude to all of them.

First of all, I would like to thank all my supervisors, Prof. Dr. Ashraf Salem, Prof. Dr. Ayman Wahba and Dr. Mona Safar. I'm very grateful for their guidance, help and endless support. Their doors were always opened for me. Without their advice and continuous assistance, this thesis had never been done. Thank you for your support to present my work in several conferences.

Dr Mona, I'm grateful to have you as my direct supervisor. Thank you for all your effort and time. Thank you for your constructive feedback. You are a wonderful researcher. You gave me chance to explore new areas.

I want to express my gratitude to the best parents I have ever seen in life. You were always there for me. You are always supporting me and believing in me during my entire life. You never gave up on me. You taught me how to develop myself, how to learn and how to achieve goals no matter are the obstacles. You sacrifices a lot during your life for me, and you are always source of happiness. Words are not enough to express my gratitude for your love and for all you did to me☺. Your positive personalities are always inspiring me.

My beloved husband and best friend, Ahmed. You are always supporting me in all the circumstances, good and bad. You are always encouraging me and pushing me to finalize this thesis. I can't thank you enough for your love, kindness, sacrifices and patience. I'm always feeling gratitude to have you in my life. You were always doing your best to cheer me up when I feel down. During the last 2 years, you were always bringing me so much joy and hope.

To my sister Nevine, I wish you would be here with me, but I'm certain you are in a better place. During 23 years, you were my soul mate and best friend. You taught me how to be grateful, how to educate myself, how to be kind, and how to be patient. You were always believing in me. You were always a good advisor. You were my mentor. Until we meet, I will always feel grateful that I had a sister and best friend like you.

To my entire big family (especially Nermine, aunt Hoda and Aunt Mona), thank you for your encouragement and support. Thank you for your understanding when I was isolated to work on the thesis.

To my closest friend Eman El Mandouh, words are not enough to show you my gratitude to have you in my life. You were always motivating me, lifting me up when I was down and supporting me. Thank you so much for pushing me to achieve this goal. Without your support and guidance, I wouldn't have done this thesis.

For all my closest friends, Shaimaa, Sohaila, Hemmat, Hanan and Dr. Yousra thank you for your support. Thank you for you constant love and help. I can't imagine my life without your precious friendship. You are wonderful friends.

To my friends and brothers, Haytham, Khaled and Wael, Thank you so much for your support. I deeply appreciate your encouragement to me. You were always by me, especially when I feel down.

To all my friends in Mentor Graphics, I'm grateful to you all. Your support and encouragement were unforgettable. Thank you so much for your support.

Student name Nahla Mohamed Mohamed Saleh
Computer and Systems Engineering
Faculty of Engineering
Ain Shams University
Cairo, Egypt

April 2017

Contents

List of Figures xvi
List of Tables xviii
List of Abbreviations xix
Chapter 1 Introduction 1
1.1 Motivation 1
1.2 Problem Statement 3
1.3 Thesis Contribution 4
1.4 Thesis Organization 6
Chapter 2 Verification Techniques 7
2.1 Functional verification 8
2.2 Coverage Verification 10
2.2.1 Coverage Verification Test Plan 13
2.3 Simulation-based Technique 14
2.3.1 Universal Verification Methodology (UVM) 14
2.4 Formal-based Technique 17
2.4.1 Symbolic Execution 18
2.4.2 Concolic Execution 21
2.4.3 Model Checking 22
Chapter 3 Embedded Devices 29
3.1 Embedded Systems 29
3.2 Virtual Prototyping 32
3.2.1 Virtual Hardware Models 34
3.2.2 QEMU Platform 35
Chapter 4 Related Work 43
Chapter 5 Automatic Test Cases Generation on Virtual Models using Symbolic Execution 47
5.1 Automatic test case generation on QEMU-based model using SE 47
5.2 Test coverage evaluation on virtual model 54
5.2.1 Creation of Registers Set 58
5.2.2 Test Replay and State Capture Approach 58
5.2.3 Automatic Coverage Analysis and Reporting 59

5.3 Test Coverage Evaluation on Real Hardware Model 61
5.4 State Pruning 62
Chapter 6 Evaluation 65
6.1 Automatic Test Cases Generation Approach 67
6.2 Test Coverage Evaluation on Virtual Model 70
6.3 Test Coverage Evaluation on RTL 73
Chapter 7 Conclusion and Future Work 75
7.1 Conclusion 75
7.2 Future work 76
References 77