State Register Identification for Circuit Reverse Engineering

Aidan Wong | a.wong71720@gmail.com
DesCyPhy Lab
Alhambra High School | Class of 2023
USC Viterbi Department of Electrical Engineering | SHINE 2022

**INTRODUCTION**

Modern integrated circuits pass through many hands from initial design to release into the supply chain, and typically contain third party intellectual property (IP).

Often, a design will use not just individual cells but large pregenerated IP cores for which the engineer may not have source code. The only access the engineer has to the third party circuitry is the netlist after the design has been compiled and synthesized. Netlists may also be recovered from fabricated chips returned from the foundry.

In either of these cases, malicious code may have been inserted into the design, either via extra logic in a third party IP core, or changes to the design by a malicious foundry. Verification that the design functions only as intended is difficult. The DesCyPhy Lab is working towards securing next generation microelectronic chips.

**METHODS**

There are several existing state register identification algorithms for reverse engineering of finite state machines. We implement and investigate one of these algorithms (RELIC) or identification using graph neural networks (ReIGNN), with other algorithms. As opposed to other methods such as topological algorithms, RELIC-FUN utilizes functional matching.

**IMPLEMENTATION**

Two algorithms derived from the pseudocode of RELIC-FUN were implemented to obtain the desired results.

1) The first algorithm explains how we classify registers.
   a) k-feasible slice: A slice of this form is a k-feasible cut of the output Y, and we call a conforming slice of k inputs k-feasible.
   b) Sorting signals & classes
      i) All registers in the target list are our target signals;
      ii) For each target signal, we identify one k-feasible slice of it, where k is specified by users;
      iii) Functional equality between two k-slices are decided by the second algorithm, and signals with functionally equivalent k-slices will be classified into the same class;
      iv) Signals in the classes with larger size are identified as data registers, while others are identified as state registers.

2) The second algorithm defines functional equality.
   To understand whether two signals are functionally equivalent or not, we need to test them under all possible situations. Therefore, we propose three termination criteria.
   a) Different input lengths: If the input length of two slices are different, they are inequivalent;
   b) Different input permutations: If the inputs of two k-slices are different, but the simulation results are the same for all possible input patterns, they are equivalent;
   c) Simulation-based equivalence: If the inputs of two k-slices are different, but the simulation results are the same for all possible input patterns, they are equivalent.

**RESULTS & ANALYSIS**

To evaluate the performance of RELIC-FUN, we compare its predictions with the true labels of the nodes. Here k is one parameter specified by the users, and it defines how large slice of each signal will be used to test their functional equality. Two k values, 2 and 3, are used in our experiments to show how the value of k impacts the results. The sensitivity of RELIC-FUN (k=2) is 100% in all three cases, while RELIC and ReIGNN cannot achieve 100% for the gpio circuit. When reverse engineering the finite state machine (FSM) of a design, achieving 100% sensitivity is important because any missing state registers can lead to an incomplete FSM.

**NEXT STEPS**

According to the experimental results, RELIC-FUN is conservative to tell two registers are functionally equivalent, and that leads to a bad performance of balanced accuracy. Also, RELIC-FUN’s performance is sensitive to the parameter k. To overcome these challenges, we could a) Randomly select multiple possible k-slices for each target signal instead of one to avoid incomplete equality testing; b) Automatic the process of choosing the value of k.

**ACKNOWLEDGEMENTS**

I would like to express my deepest appreciation and gratitude to the following people, all of whom have made this great research experience possible...

To Professor Nuzzo who accepted me into the program and allowed me to experience electrical engineering research to Dr. Katie Mills who runs a wonderful program, allowing me to experience electrical engineering research to the friends I made here at USC who made me laugh and enjoy every moment of the internship to Ph.D. student Kaixin Yang, my mentor, who answered every question I had and gave me a lot of insight into the process and to my family who have supported and helped me along the way in my journey to becoming an engineer.