PLEASE TYPE

THE UNIVERSITY OF NEW SOUTH WALES

Thesis/Dissertation Sheet

Surname or Family name: Legg		
First name: Alexander	**Other name/s: Jonathan**	
Abbreviation for degree as given in the University calendar:	**PhD**	
School: Computer Science and Engineering	**Faculty: Engineering**	
Title: A Counterexample Guided Method for Reactive Synthesis		

Abstract 350 words maximum: (PLEASE TYPE)

Software controllers of reactive systems are ubiquitous in situations where incorrectness has a high cost. In order to place trust in the software, strong guarantees of its functional correctness are required. Reactive synthesis can be used to automatically construct software to a specification and ensure correctness. The drawback is that synthesis is computationally hard and it is infeasible to synthesise a controller for many specifications.

Synthesis is formalised as a game between the controller and its environment. In this thesis we consider safety specifications that define the winning condition of the game for the controller as never allowing the game to visit an error state. The usual approach for solving controller synthesis is to compute the set of all winning states in the system and construct a controller that never deviates from this set. The set may be very large so it is standard practice to represent sets of states symbolically as a relation over the variables of the system. Binary decision diagrams (BDDs) are an efficient data structure used to store and manipulate sets of states for synthesis. The drawback of this approach is that a set of states has only one representation as a BDD and in some cases it may be exponentially large in the number of variables. The state explosion of BDDs causes controller synthesis to be infeasible on specifications with no compact representation of the set of winning states.

In this thesis I propose a synthesis algorithm that constructs an approximation of the set of safe states that is sufficient to show correctness of the controller. The algorithm constructs an abstraction of the game and searches for a candidate strategy for the controller. Counterexamples are used to refine the strategy until it is winning for the game abstraction. Similar to bounded model checking, a SAT solver is used to efficiently implement the search for a counterexample trace. When a strategy is found to be winning in the abstraction of the game an approximation of the states for which the strategy wins is extracted from the strategy via interpolation. The search continues by refining the abstraction until the approximation of winning states converges on a fixed point that is sufficient to prove that the specification is realisable.

.....	.....	.....
Signature	**Witness Signature**	**Date**

The University recognises that there may be exceptional circumstances requiring restrictions on copying or conditions on use. Requests for restriction for a period of up to 2 years must be made in writing. Requests for a longer period of restriction may be considered in exceptional circumstances and require the approval of the Dean of Graduate Research.

FOR OFFICE USE ONLY	**Date of completion of requirements for Award:**	

THIS SHEET IS TO BE GLUED TO THE INSIDE FRONT COVER OF THE THESIS