Untitled CAV Paper

Alexander Legg[1], Leonid Ryzhyk[2], and Nina Narodytska[2]

[1] NICTA* and UNSW
alexander.legg@nicta.com.au
[2] Samsung Research

Abstract. This is the abstract

1 Introduction

Reactive systems are ubiquitous in real-world problems such as circuit design, industrial automation, or device drivers. Automatic synthesis can provide a *correct by construction* controller for a reactive system from a specification. However, the reactive synthesis problem is 2EXPTIME-complete so naive algorithms are infeasible on even simple systems.

Reactive synthesis is formalised as a game between the *system* and its *environment*. In this work we focus on safety games, in which the system must prevent the environment from forcing the game into an error state. Much of the complexity of reactive synthesis stems from tracking the set of states in which a player is winning.

There are several techniques that aim to mitigate this complexity by representing states symbolically. Historically the most successful technique has been to use *Binary Decision Diagrams* (BDDs). BDDs efficiently represent a relation on a set of game variables but in the worst case the representation may be exponential. This means that BDDs are not a one-size-fits-all solution for all reactive synthesis specifications.

Advances in SAT solving technology has prompted research into its applicability to synthesis as an alternative to BDDs. One approach is to find sets of states in CNF [**?**]. Another approach is to eschew states and focus on *runs* of the game. Previous work has applied this idea to solving bounded games [**?**] by forming abstract trees of individual runs. In this paper, we extend this idea to unbounded games by constructing approximate sets of winning states from abstract trees.

2 Reactive Synthesis

* NICTA is funded by the Australian Government as represented by the Department of Broadband, Communications and the Digital Economy and the Australian Research Council through the ICT Centre of Excellence program.