Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 309 (2014) 63–74

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Bounded Model Checking of Traffic Light Control System

Bin Yu[1,2] Zhenhua Duan*, Cong Tian[3]

Institute of Computing Theory and Technology, and ISN Lab
Xidian University
Xi'an, P.R.China

Abstract

Traffic Light Control System (TLCS) is widely used in our daily life. It is of great importance to ensure the correctness of TLCS. In this paper, bounded model checking (BMC) is chosen to verify a simple but practical TLCS. To this end, Propositional Projection Temporal Logic (PPTL) used as the property specification language and the process of BMC for PPTL are briefly introduced. Then, a TLCS is described and its corresponding Kripke structure is given. Finally, two related properties specified by PPTL formulas are verified for the system using the BMC approach. The verification result using our bounded model checker, BMC4PPTL, shows that the behavior of TLCS is consistent with the specification.

Keywords: Bounded Model Checking, PPTL, TLCS, Verification

1 Introduction

Techniques for automatic formal verification of finite state transition systems have been studied in recent years. The most widely used approach is called Model Checking [4,6]. As a trusted, strong and automatic verification technique, model checking has been widely used in many fields such as verification of hardware, software and communication protocols. With model checking, the system to be verified is modeled as a finite state machine and the specification is formalized in terms of temporal logic formulas. In practice, linear-time temporal logic (LTL) [16] and branching-time temporal logic (CTL) [4] are popular.

[1] This research is supported by the National Program on the Key Basic Research Project of China (973 Program) under Grant No. 2010CB328102, and the National Natural Science Foundation of China under Grant Nos. 61133001, 61272117, 61272118, 61202038, 91218301, 61322202 and 61373043. * Corresponding author.

[2] Email: yubin9011@126.com

[3] Email: zhhduan,ctian@mail.xidian.edu.cn

http://dx.doi.org/10.1016/j.entcs.2014.12.006

SPIN [14] based on LTL and SMV [15] depended on CTL are two well-known model checkers. However, as known, automata-based model checking algorithms can easily lead to state space explosion when the number of states in the system is large. To fight this problem, several approaches, such as Symbolic Model Checking (SMC) [2], Abstract Model Checking (AMC) [5], and Compositional Model Checking [7], have been proposed with success. The combination of SMC with BDDs [15,8] pushed the barrier to systems with 10^{20} states and more [2]. But the bottleneck of SMC is the amount of memory that is required for storing and manipulating BDDs. The boolean functions required to represent the set of states can grow exponentially. Bounded model checking (BMC) is an important progress in formalized verification after symbolic model checking [1]. The basic idea of BMC is to search for a counterexample in executions whose length is bounded by some integer k. If the property is not satisfied, an error is found. Otherwise, we cannot tell whether the system satisfies the property or not. In this case, we can consider increasing k, and perform the process of BMC again. The BMC problem can be efficiently reduced to a propositional satisfiability problem, and can therefore be solved by SAT solvers rather than BDDs. Modern SAT solvers can handle propositional satisfiability problems with hundreds of thousands of variables.

With model checking and bounded model checking, the mostly used temporal logics are LTL, CTL and their variations. However, the expressiveness of LTL and CTL is not powerful enough, actually, not full regular. There are at least two types of properties in practice which cannot be specified by LTL and CTL: (1) some time duration related properties such as a property P holds after 100^{th} time unit and before 200^{th} time unit; (2) some periodically repeated properties P. Propositional Projection Temporal Logic (PPTL)[9,11] is a useful formalism for specification and verification of concurrent systems. The expressiveness of PPTL is full regular [17] which allows us to verify full regular properties and time duration related properties of systems in a convenient way.

To combine the advantages of BMC and PPTL, the bounded semantics of PPTL formulas and the process of BMC for PPTL have been presented in [12]. The bounded model checker for PPTL named BMC4PPTL has been developed so that automatical verification can be conducted. With BMC4PPTL, we describe the model by the input language used in NuSMV [3] and specify the property by a PPTL formula. When a PPTL formula R is a chop construct in the form of $R \equiv Q_1; Q_2$, R is false if Q_1 only has infinite models and we don't consider this case in this paper.

In our daily life, TLCS plays an important role to make the traffic be safe and efficient. So it is of great importance to ensure the correctness of TLCS. In this article, first we describe a TLCS by a Kripke structure M according to the requirement specification. Then one safety property and one periodically repeated property to be verified are specified by PPTL formulas. After that, the BMC approach is employed to find a counterexample. The verification is done automatically by BMC4PPTL and the results show that the system is consistent with the specification.

This paper is organized as follows. The next section presents the preliminaries, including the Kripke structure used for the description of a model and the property