Symbolic Model-Checking Method Based on Approximations and Binary Decision Diagrams for Real-Time Systems

Satoshi Yamane  Kazuhiro Nakamura

Department of Computer Science, Faculty of Science, The University of Shimane
1060 Nishikawatu, Matsue City, Japan, 690
E-mail: yamane@cis.shimane-u.ac.jp

Abstract

Real-time systems can be described using the timed automata of Alur and Dill. Although there exist model-checking algorithms for timed automata, the problem is intractable (PSPACE-complete). In this paper, we propose a model-checking method based on approximations and symbolic representations. We recursively refine over- and underapproximations to compute the set of states that satisfy a temporal formula. The approximate sets are represented using a combination of BDDs (Binary Decision Diagrams) and DBMs (Difference Bound Matrices). We have developed a verification tool based on this method. As a case study, we check safety and liveness properties of an Ethernet protocol.

1 Introduction

In real-time systems, the computer interacts with physical processes for which time is an important factor. Thus the design of these real-time systems must consider not only the sequencing and coordination of events, but also the times at which they occur. Any formal methodology for specifying and reasoning about such real-time systems as protocols and circuits must include an accurate model of timed behavior. Real-time systems have been formalized by Alur-Dill's timed automata [1]. Since then, many formal automatic verification methods of real-time systems have been proposed such as model-checking, language inclusion, and bisimulation check, etc.

In this paper, we focus on Alur-Dill's timed automata [1] and symbolic model-checking [2], and propose an efficient symbolic model-checking method based on overapproximations and underapproximations.

As the verification of timed automata is known to be PSPACE-complete [3], it is essentially an intractable problem. Several verification methods have been developed in order to reduce verification costs as follows.

1. Henzinger [4] et al. have proposed the method based on symbolically representing regions as state predicates instead of constructing full region graphs.
However, when region graphs grow large, verification costs of this method become expensive. The verifier KRONOS has been implemented by IMAG.

2. Kim Larsen [5] et al. have proposed a compositional verification method. However, verification costs of this method become too expensive to be practical if the number of clock variables increases, because the memory requirements increase according to the exponentials of the number of states and clock variables for quotient constructions. The verifier UPPAAL has been implemented at BRICS.

3. Dill and Wong-Toi [6][7] have proposed the method based on approximations. They symbolically represent both states and timing constraints of real-time systems by BDDs(Binary Decision Diagrams) [8] and DBMs(Difference Bounds Matrices) [9][10]. They use approximations to avoid wasting a huge memory. Hence, the method is advantageous in verification costs, and it is applicable to verify a large scale of real-time systems. However, we can verify only the safety property (AG¬p) by this method. The verifier Veriti has been implemented at Stanford University.

In this paper, we propose the symbolic model-checking method based on recursive overapproximations and underapproximations, extending the approximations method of Dill and Wong-Toi. The method enables us to verify real-time systems using temporal logic formulas such as EU, EG and EF. Our proposed method is different from the reachability method proposed in [7]. In general, symbolic model-checking is realized by recursively computing a set of states in which subformulas hold. In analysis of real-time systems, it is effective to represent sets of states using BDDs. But, as each timing constraint is different in each state, approximations are required. We propose the algorithms of approximations for a greatest fixpoint and a least fixpoint. A verifier SVAX (Shimane Verifier based on Approximations) is implemented using our proposed method. We apply SVAX to verify the safety and liveness properties of the Ethernet protocol.

Outline
The remainder of the paper is organized as follows. In the next section, we give the specification language to specify real-time systems by timed Kripke structures and verification properties by temporal logic. In Section 3, we propose symbolic model-checking method based on approximations of combining BDDs and DBMs. In Section 4, we give some experimental results to show the effectiveness of this method by our verification system SVAX. Moreover, we compare SVAX with other symbolic verifiers such as KRONOS, UPAAAL and Veriti. Section 5 concludes the paper.