Checking ACTL* Properties of Discrete Timed Automata via Bounded Model Checking*

Bożena Woźna and Andrzej Zbrzezny

Institute of Mathematics and Computer Science
PU of Częstochowa
Armii Krajowej 13/15, 42-200 Częstochowa, Poland
{b.wozna,a.zbrzezny}@wsp.czest.pl

Abstract. The main contribution of the paper consists in showing that the BMC method is feasible for ACTL* (the universal fragment of CTL*) which subsumes both ACTL and LTL. The extension to ACTL* is obtained by redefining the function returning the sufficient number of executions over which an ACTL* formula is checked, and then by combining two known translations to SAT for ACTL and LTL formulas. The proposed translation of ACTL* formulas is essentially different from the existing translations of both ACTL and LTL formulas. Moreover, ACTL* seems to be the largest set of temporal properties which can be verified by means of BMC. We have implemented our new BMC algorithm for discrete timed automata and we have presented a preliminary experimental results, which prove the efficiency of the method. The formal treatment is the basis for the implementation of the technique in the symbolic model checker verics.

1 Introduction

Model checking is considered as one of the most spectacular practical applications of the theoretical computer science in verification of concurrent systems. The main idea of model checking consists in representing a program as a labeled transition system (model), representing a specification as a temporal formula, and checking automatically whether the formula holds in the model [10]. Unfortunately, the practical applicability of model checking is strongly restricted by the state explosion problem, which is mainly caused by representing concurrency of operations by their interleaving. Therefore, many different reduction techniques have been introduced in order to alleviate the state explosion. The major methods include application of partial order reductions [4, 21, 22, 28], symmetry reductions [15], abstraction techniques [12, 11], BDD-based symbolic storage methods [19], and SAT-related algorithms [2, 6, 9, 14, 18, 20, 23, 24, 25, 26, 29].

* Partly supported by the State Committee for Scientific Research under the grant No. 8T11C 01419.
Bounded model checking (BMC) based on SAT (satisfiability checking) methods has been introduced as a complementary technique to BDD-based symbolic model checking for LTL [6, 7]. The main idea of bounded model checking for LTL is to look for an execution of the system of some length $k$, which is a counterexample for a tested property. If no counterexample of length $k$ can be found, then $k$ is increased by one. The efficiency of this method is based upon an observation that if a system is faulty, then often only a (small) fragment of its state space is sufficient for finding an error. The above observation has been experimentally proved [6, 7, 23, 25].

The main contribution of our paper is an extension of the method BMC to verification of the branching time properties expressible in ACTL$^*$ (the universal fragment of CTL$^*$) [10], which subsumes both ACTL and LTL. ACTL$^*$ seems to be the largest set of temporal properties which can be verified by means of BMC. Moreover, we have implemented our new BMC algorithm for Discrete Timed Automata [8] and proved its efficiency by performing several experiments for the standard mutual exclusion protocol. The proposed BMC algorithm for ACTL$^*$ is going to be a new module of the tool √erics [13].

The main idea of our new BMC method for ACTL$^*$ consists in combining a translation of a model $M$ to several symbolic paths, which can start at arbitrary states of the model, with a translation of the negation of an ACTL$^*$ formula $\varphi$. The latter translation is obtained by redefining the function $f_k$ of [23] returning the sufficient number of executions over which $\varphi$ is checked, and then by combining two known translations for ACTL [23] and LTL [6]. This is obtained by applying the LTL translation for all the LTL subformulas of $\varphi$, and the ACTL translation for all the state subformulas of $\varphi$, i.e., the formulas which begin with a path quantifier.

The rest of the paper is organized as follows. The next section contains the discussion of the related work. Then, in section 3 the bounded model checking for ACTL$^*$ is presented. The implementation of BMC for Discrete Timed Automata is described in section 4. Experimental results are presented in section 5. The last section contains final remarks.

2 Related Work

Our paper shows for the first time an extension of the BMC method based on SAT procedures to verification of all the properties expressible in ACTL$^*$. It builds upon the results of [23], where an approach to applying BMC for ACTL was described. The idea of BMC for a temporal logic is taken from [6, 7]. The BMC method has been also applied for LTL model checking of 1-safe Petri Nets [18] and Timed Automata [2], for TACTL model checking of Timed Automata [25, 24], for checking reachability of Petri Nets [17] and Timed Automata [20, 26, 29], for past LTL model checking of digital circuits [3]. A motivation for considering the universal fragment of CTL$^*$ can be found in [16, 22]. The discrete timed automata were considered by several authors [8, 5] because the model checking of such automata is a very challenging and important task.