Streszczenie

Celem tej rozprawy doktorskiej jest opracowanie bazujących na testerach SAT i SMT algorytmów ograniczonej weryfikacji modelowej (BMC) dla systemów współbieżnych, systemów czasu rzeczywistego i systemów wieloagentowych. Ponadto, celem jest również porównanie algorytmów ograniczonej weryfikacji modelowej bazujących na testerach SAT z odpowiadającymi metodami bazującymi na testerach SMT.

Automatyczna weryfikacja systemów wykonywana poprzez analizę ich modeli jest bardzo ważnym tematem badań. Motywację dla tych badań stanowi rosnące zapotrzebowanie na testowanie krytycznych systemów bezpieczeństwa, takich jak systemy zależne od czasu, których awaria może spowodować dramatyczne konsekwencje dla ludzi i sprzętu.

Znaczna część badań obejmuje rozwój bazującej na SMT metodzie BMC dla standardowych struktur Kripkego, rozszerzonych struktur Kripkego i dla wagowych systemów interpretowanych dla różnych wagowych temporalnych języków przeznaczonych do specyfikowania własności systemów. Każdy z tych języków zostanie także rozszerzony o standardowe operatory epistemiczne.

Ograniczona weryfikacja modelowa jest techniką weryfikacji zaprojektowaną do znajdywania kontrprzykładów. Została ona zaproponowana jako uzupełnienie techniki stosującej Binarne Diagramy Decyzyjne (BDD), a jej celem było przede wszystkim złagodzenie problemu eksplozji stanów. Podstawowa idea metody BMC polega na tym, że mając dany model $\mathcal{M}$, własność P oraz ograniczenie k będące liczbą naturalną, BMC rozwija system $\mathcal{M}$ do głębokości k i transluje to rozwinięcie oraz badaną własność do formuły F, takiej że F jest spełnialna wtedy i tylko wtedy, gdy P jest prawdziwa w modelu $\mathcal{M}$ na głębokości mniejszej lub równej k. Aby sprawdzić, czy formuła F jest spełnialna stosuje się testery spełnialności zdaniowej (SAT-testery) lub testery spełnialności względem wybranej teorii (SMT-testery). Dla BMC bazującej na SAT F jest formułą zdaniową, której spełnialność jest sprawdzana przez przez SAT-tester, natomiast dla BMC bazującej na SMT F jest bezkwantyfikatorową formułą pierwszego rzędu, której spełnialność jest sprawdzana przez przez SMT-tester.

Słowa kluczowe: *ograniczona weryfikacja modelowa, SAT, SMT, systemy współbieżne, systemy czasowe, systemy wieloagentowe*

Abstract

The aim of this Ph.D. thesis is to investigate the foundations of novel SAT- and SMT-based bounded model checking (BMC) algorithms for concurrent, real-time and multi-agent systems. Moreover, the aim is to compare the SAT-based bounded model checking algorithms with the corresponding SMT-based bounded model checking techniques.

Automated verification of systems performed by the analysis of their models is a very important subject of research. This is highly motivated by an increasing demand to verify safety critical systems, i.e., time-dependent systems, failure of which could cause dramatic consequences for both people and hardware.

A major part of the research involve the development of SMT-based BMC methods for standard Kripke structures, extended Kripke structures, and for weighted interpreted systems for different weighted temporal languages, each of which will be augmented to include the standard epistemic operators.

Bounded model checking is a verification technique designed for finding counterexamples. It has been introduced as a complementary technique to Binary Decision Diagrams (BDD's) for alleviating the state explosion problem. The basic idea of the BMC technique is to check a given existencial property at a given depth. Namely, given a model $\mathcal{M}$, a property P, and a bound k (a natural number), BMC unrolls the system k times and translates it into a formula F such that F is satisfiable if and only if P has a witness of depth less than or equal to k. To check whether F is satisfiable, either standard Boolean satisfiability solvers (SAT-solvers), or Satisfiability Modulo Theories solvers (SMT-solvers) can be used. In SAT-based BMC F is a propositional formula, which is then checked for satisfiability by a SAT solver, and in SMT-based BMC F is a quantifier-free first order formula, which is then checked for satisfiability by an SMT solver.

Keywords: *bounded model checking, SAT, SMT, concurrent systems, timed systems, multi-agent systems*