CEGAR-alapú verifikációs algoritmusok időzített automaták ellenőrzésére

A napjainkban egyre inkább elterjedő biztonságkritikus rendszerek hibás működése súlyos károkat okozhat, emiatt kiemelkedően fontos a matematikailag precíz ellenőrzési módszerek alkalmazása a fejlesztési folyamat során. Ennek egyik eszköze a formális verifikáció, amely már a fejlesztés korai fázisaiban képes felfedezni tervezési hibákat. A biztonságkritikus rendszerek komplexitása azonban gyakran megakadályozza a sikeres ellenőrzést, ami különösen igaz az időzített rendszerekre: akár kisméretű időzített rendszereknek is hatalmas vagy akár végtelen állapottere lehet. Ezért különösen fontos a megfelelő modellezőeszköz valamint hatékony verifikációs algoritmusok kiválasztása. Az egyik legelterjedtebb formalizmus időzített rendszerek leírására az időzített automata, ami a véges automata formalizmust óraváltozókkal egészíti ki, lehetővé téve az idő múlásának reprezentálását a modellben.

Formális verifikáció során fontos kérdés az állapotelérhetőség, amely során azt vizsgáljuk, hogy egy adott hibaállapot része-e az elérhető állapottérnek. A probléma komplexitása már egyszerű (diszkrét változó nélküli) időzített automaták esetén is exponenciális, így nagyméretű modellekre ritkán megoldható. Ezen probléma leküzdésére nyújt megoldást az *absztrakció* módszere, amely a releváns információra koncentrálva próbál meg egyszerűsíteni a megoldandó problémán. Az absztrakció-alapú technikák esetén a fő probléma a megfelelő pontosság megtalálása. Az ellenpélda vezérelt absztrakciófinomítás (*counterexample-guided abstraction refinement, CEGAR*) iteratív módszer, amely a rendszer komplexitásának csökkentése érdekében egy durva absztrakcióból indul ki és ezt finomítja a kellő pontosság eléréséig.

Munkám célja hatékony algoritmusok fejlesztése időzített rendszerek verifikációjára. Munkám során az időzített automatákra alkalmazott CEGAR-alapú elérhetőségi algoritmusokat vizsgálom és közös keretrendszerbe foglalom, ahol az algoritmusok komponensei egymással kombinálva új, hatékony ellenőrzési módszerekké állnak össze. Az irodalomból ismert algoritmusokat továbbfejlesztettem és hatékonyságukat mérésekkel igazoltam.

CEGAR-based verification algorithms for model checking timed automata

Nowadays safety-critical systems are becoming increasingly popular, however, faults in their behavior can lead to serious damage. Because of this, it is extremely important using mathematically precise verification methods during their development. One of these methods is formal verification that is able to find design problems since early phases of the development. However, the complexity of safety-critical systems often prevents successful verification. This is particularly true for real-time systems: even small timed systems can have large or even infinite states pace. Because of this, selecting an appropriate modeling formalism and efficient verification algorithms is very important. One of the most common formalism for describing timed systems is the timed automaton that extends the finite automaton with clock variables to represent the elapse of time.

When applying formal verification, reachability becomes an important aspect – that is, examining whether or not the system can reach a given erroneous state. The complexity of the problem is exponential even for simple timed automata (without discrete variables), thus it can rarely be solved in case of large models. Abstraction can provide assistance by attempting to simplify the problem to solve while focusing on the relevant information. In case of abstraction-based techniques the main difficulty is finding the appropriate precision. Counterexample-guided abstraction refinement (CEGAR) is an iterative method starting from a coarse abstraction and refining it until the sufficient precision is reached.

The goal of my work is to develop efficient algorithms for verification of timed automata. In my work I examine CEGAR-based reachability algorithms applied to timed automata and I integrate them to a common framework where components of different algorithms are combined to form new and efficient verification methods. I improved known algorithms and proved their effectivity by measurements.

Munkám célja időzített automatákra alkalmazott elérhetőségi algoritmusok implementálása és közös CEGAR keretbe foglalása, hogy azok egyes komponensei egymással kombinálva új, hatékony algoritmusokká álljanak össze. Az irodalomban található algoritmusokat általam fejlesztettekkel egészítettem ki. Kitaláltam egy olyan CEGAR-alapú algoritmust, ami nem az automatát, hanem közvetlenül az állapotteret finomítja. Megalkottam egy olyan megközelítést, amely segítségével

Az irodalomban számos algoritmus található időzített automaták verifikálására, melyek közül saját algoritmusom alapjául egy széles körben elterjedt, hatékony modellellenőrző, az *Uppaal* algoritmusa szolgál. Ennek különlegessége, hogy egy hatékony absztrakciót, úgynevezett *zónaákat* használ a folytonos, így végtelen állapottér reprezentálására.

Dolgozatomban bemutatok egy új CEGAR-alapú megközelítést, amely lehetővé teszi időzített automatákkal leírt valósidejű rendszerek formális verifikációját. Az algoritmus (beleértve az Uppaal modellellenőrző algoritmusát) az implementálhatóság biztosítása érdekében részletesen bemutatásra kerül, az érthetőség megkönnyítése érdekében pedig egy példán is illusztrálva van. A dolgozat tárgyalja az algoritmus alkalmazhatóságát is, így bemutatja az előnyeit a korábbi, hasonló megoldásokhoz képest, valamint bizonyítást ad az algoritmus helyességére és terminálódására.