Időzített rendszerek CEGAR alapú analízise

A valósidejű biztonságkritikus rendszereken alkalmazott formális verifikáció képes felfedezni tervezési hibákat a fejlesztés különböző fázisaiban. Azonban a formális módszerek nagy számításigénye gyakran gátat szab a sikeres verifikációnak.

Az *absztrakció* módszerét gyakran alkalmazzák egyszerű, hatékonyan verifikálható modellek megalkotására, az ellenpélda vezérelt absztrakciófinomítás (*counterexample-guided abstraction refinement, CEGAR*) iteratív módszere segítségével pedig megválasztó a megfelelő szintű absztrakció.

A hatékony verifikációhoz fontos a megfelelő modellezőeszköz megválasztása. 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.

Az irodalomban sokféle 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.