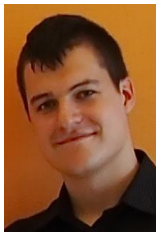
Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

CEGAR-alapú modellellenőrzés vizsgálata



Hajdu Ákos, II. évf, (MSc) mérnök inf. szakos hallgató
Konzulens: Vörös András tudományos segédmunkatárs, MIT
Szolgáltatásbiztos rendszertervezés szakirány
Diplomatervezés 1 összefoglaló
2014/15. II. félév

Manapság a formális modellezés és verifikáció a hibamentesség igazolásának egyre inkább elterjedt eszköze, különösen a komplex, elosztott és biztonságkritikus rendszerek esetében. A rendszerek modelljeit általában valamilyen magasabb szintű formalizmusban írják le, amely a mérnöki szemléletmódhoz közel áll. Ezen modellek viselkedését az elérhető állapotok és állapotátmenetek halmaza, azaz az állapottér adja meg. A modellellenőrzés egy olyan formális verifikációs algoritmus, amely az állapottér bejárásával képes automatikusan ellenőrizni temporális logikai követelmények teljesülését. A modellellenőrzés egyik nagy hátránya azonban az állapottér robbanás. Egészen kicsi rendszereknek is lehet hatalmas, vagy akár végtelen nagy állapottere. A probléma leküzdésére számos megoldás született: szimbolikus módszerek, részleges rendezés alapú redukció, korlátos modellellenőrzés, absztrakció.

Diplomaterv 1 munkám során egy absztrakció alapú módszert, az úgynevezett ellenpélda alapú absztrakció finomítást (CEGAR) vizsgáltam. A módszer lényege, hogy a modellt bizonyos megkötések elhagyásával egyszerűsíti, így egy olyan absztrakt modellt vizsgál, ami felülbecsli az eredetit. A felülbecslésből adódóan az eredeti modell minden viselkedését megtartja, így ha egy követelmény teljesül, akkor az az eredeti modellben is. Ugyanakkor, ha egy követelmény nem teljesül, akkor ezt okozhatják az absztrakció durvasága miatt behozott új viselkedések is. Ilyen esetekben az absztrakció finomítására van szükség. A CEGAR alapú algoritmusok általában egy kicsi állapotterű, durva absztrakcióból indulnak ki és addig finomítják, amíg a követelmény nem teljesül, vagy egy valódi ellenpéldát nem találnak.

Eddigi munkám során feldolgoztam a szakirodalom legfontosabb cikkeit a CEGAR megközelítésről és két különböző megközelítést alkalmazó algoritmust implementáltam a tanszéki TTMC modellellenőrző keretrendszerbe.

- Az egyik megközelítés a rendszerben lévő változók csoportosítására (klaszterezésére) épít. Minden változócsoporthoz elkészít egy absztrakt modellt, majd ezek kompozícióján végzi el a modellellenőrzési feladat egy speciális esetét, az elérhetőségi analízist. A megtalált ellenpéldát SMT megoldó segítségével szimulálja az eredeti modellben. Amennyiben az ellenpélda nem hajtható végre, valamely változócsoportokhoz tartozó absztrakt állapotteret (állapottereket) finomítja.
- A másik megközelítés predikátum absztrakcióra épít. Egy tetszőlegesen megadott kezdeti predikátumlista alapján elkészít egy modellt, majd ezen vizsgál elérhetőséget. A megtalált ellenpéldát ez a megoldás is SMT megoldó segítségével szimulálja. Nem végrehajtható ellenpélda esetén interpolánsok segítségével finomítja az absztrakt állapotteret.

A további munkám célja, hogy megvizsgáljam az algoritmusok hatékonyságát és továbbfejlesztéseket, kiterjesztéseket javasoljak.