Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

Szoftver verifikáció absztrakciós módszerek kombinálásával

Bajkai Viktória Dorina III. évf, BSc mérnökinformatika szakos hallgató
Konzulens: Hajdu Ákos
Rendszertervezés specializáció
Önálló laboratórium összefoglaló
2017/18. II. félév

Biztonságkritikus rendszerek esetén nagy az igény arra, hogy bizonyítékot adjunk a program helyes működésére. A modellellenőrzés egyike a jellegzetes szoftver ellenőrzési technikáknak, használatával precíz, pontos eredményt kaphatunk, hátránya viszont a nagy számítási igényük. Ezen probléma elkerülésének egy gyakran alkalmazott módszere az ellenpélda-alapú absztrakció finomítás (CEGAR). A féléves munkám során két, a CEGAR algoritmuscsaládba tartozó módszerrel, az Explicit változó analízissel és a Predikátumabsztrakcióval ismerkedtem meg.

A kitűzött feladatom egy olyan szorzat absztrakció létrehozása volt, ami egyszerre alkalmazza az Explicit változó analízis és a Predikátumabsztrakció algoritmusokat, mindkettőnek az előnyeire fókuszálva. A cél az volt, hogy az új algoritmus minél gyorsabban és minél több modellt verifikáljon, az előzőeknél hatékonyabban.

A két absztrakciós algoritmus kombinálásakor az volt a fő feladat, hogy az új algoritmus hogyan döntse el, hogy finomításkor Explicit változó analízist, vagy Predikátumabsztrakciót alkalmazzon. A félév során több féle algoritmust is írtam, mindezt a Theta tanszéki keretrendszerben implementálva.

Az elkészült programot több mint 430 iparilag releváns példán futtattuk, különböző algoritmusokkal, beállításokkal. A végső algoritmussal jó eredményeket értünk el, jóval több modellre futott le, mint az Explicit változó analízis, és gyorsabban, mint a Predikátumabsztrakció.