Modelltranszformációk verifikációja

Önálló laboratórium feladat összefoglalója (2. félév)

Ujhelyi Zoltán (FEJLU4)
Konzulens: Horváth Ákos, Varró Dániel
BME Méréstechnika és Információs Rendszerek Tanszék
Informatikai infrastruktúra tervezése szakirány, 2007/2008. II. félév

Napjainkban a beágyazott biztonságkritikus rendszerek egyre szélesebb körben való terjedésének következtében (autóipar, folyamatirányítás, repülőgépipar) igényként merült fel a komponensek minél gyorsabb és olcsóbb fejlesztése. Ezen problémákra jelent megoldást a modellvezérelt rendszertervezés adoptálása, amely platformfüggetlen modellekből indulva transzformációs lépések sorozatával ér el a futtatható kód szintjére.

A különböző biztonságkritikus szabványoknak való megfelelőség egyre komolyabb igényt támaszt a fejlesztés során alkalmazott transzformációk helyességének ellenőrzésére, bizonyítására. Ezzel biztosítva például azt, hogy a különböző modelleken elvégzett verifikációs vagy validációs lépések során előkerülő hibák nem a transzformációk végrehajtása közben kerültek a modellbe.

Az önálló labor célja az volt, hogy az előző félévben megismert, efféle transzformációk vizsgálatához használható technológiákat részletesebben megismerjem, illetve egy hasonló célra használható eszköz fejlesztését megkezdjem.

A korábban megismert, Microsoft Research által fejlesztett Spec# keretrendszert tovább teszteltem. Ennek érdekében a már megkezdett egyszerű mintaprogram fejlesztését és statikus ellenőrzését folytattam.

Ezzel a keretrendszerrel azt tudjuk megvizsgálni, hogy az implementált transzformáció megfelel-e a transzformáció specifikációjának. Más szempontból tekintve a problémakört hasznos lehet még a forrás- és célmodellek metamodelljei felett ellenőrizni a transzformáció helyességét. Az értelme a metamodelleken történő vizsgálatnak, hogy bármilyen tulajdonságot tudunk itt mondani a transzformációról, az az összes illeszkedő metamodellen is teljesülne.

A metamodellek verifikációjához a transzformációs lépések választásához felhasznált absztakt állapotgép vizsgálatára alkalmas program fejlesztése kezdődött el a félév során. A fejlesztés első célja, hogy ezen absztrakt állapotgép program típushelyességét igazolni lehessen.

A helyesség igazolásakor arra az alapvető megfigyelésre építünk, hogy az absztrakt állapotgép kódjában található változókiértékelések, illetve vezérlési szerkezetek különféle korlátozásokat jelentenek a felhasznált változók típusára, és ezeket a megszorításokat összegyűjtve, és ezekből következtetve potenciális hibákat lehet detektálni. Ez a megfigyelés azért hasznos, mert az ebben a formában megadott adatok ellentmondásmentességét CSP (Constraint Satisfaction Problem, magyarul kényszerkielégítési probléma) megoldó segítségével lehet ellenőrizni.

Ehhez a Gecode/J nevű CSP megoldót ismertem meg és teszteltem a teljesítmény vonatkozásában. A teszt eredménye megfelelő volt, várhatóan az ellenőrzés sebessége megfelelő ahhoz, hogy azt az állapotgép írása közben a programozó segítségnek használhassa fel.

A laboratórium folytatásaként azt tervezem, hogy ezt az ellenőrzőt megvalósítom, és integrálom a tanszéken fejlesztett Viatra modelltranszformációs keretrendszerbe.