Modelltranszformációk verifikációja (Design by contract)

Önálló laboratórium feladat összefoglalója (1. félév)

Ujhelyi Zoltán (FEJLU4)
Konzulens: Horváth Ákos, Varró Dániel
BME Méréstechnika és Információs Rendszerek Tanszék
Informatikai infrastruktúra tervezése szakirány , 2007/2008. I. 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 ezen transzformációk vizsgálatához használható módszereket és eszközöket ismerjek meg részleteiben.

Ilyen módszer a Bertrand Meyer által bevezetett design by contract metodológia. A megközelítés alapja, hogy bebizonyítsuk, hogy az előfeltételben foglalt feltételek igaz értéke esetén fennáll az utófeltételben foglalt állítás is. Ezen elveket a gráftranszformációra vetítve egy baloldal felfogható egy szerződés előfeltételének, míg egy jobboldal az utófeltételének, így lehetőség nyílik arra, hogy csupán a transzformációs szabályok metamodellek felett vett leírását felhasználva modellfüggetlen helyességbizonyításokat végezhessünk.

Az ezirányú vizsgálatok elvégzésének implementációjára a Microsoft Research által fejlesztett Spec# keretrendszert használnám, ehhez szükséges volt a rendszer alaposabb megismerése és tesztelése. Ennek érdekében egy egyszerű mintaprogram fejlesztése és e mintaprogramon a statikus ellenőrzési lehetőségek tesztelését hajtottam végre.

Ezzel a keretrendszerrel azt tudjuk megvizsgálni, hogy az implementált transzformáció megfelel-e a transzformáció specifikációjának. Más szempontból vizsgálva a problémakört hasznos lehet még a forrás- és célmodellek metamodelljei felett vizsgálni 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 verifikációja céljából több különböző módszertan leírását tanulmányoztam át. Ezek közül a leglényegesebbek a Jörg Bauer által bevezetett Topology Abstraction, valamint az Ole Agesen nevéhez fűződő Constraint-based Type Inference eljárások. A Topology Abstraction célja az, hogy a modellteret felülről becsülve úgy csökkentse a komplexitást, hogy közben az ellenőrzés helyessége garantálható. A Constraint-based Type Inference módszer pedig arra tesz kísérletet, hogy a nem típusos (esetleg gyengén típusos) nyelveken írt programok esetén is lehessen ellenőrzést végezni a típusok helyességének megállapítására.

A laboratórium folytatásaként a megismert technikákat szeretném már ténylegesen modelltranszformációk ellenőrzésére felhasználni, esetlegesen meglevő Viatra modelltranszformációs keretrendszerbe integrálni.