

Automatikus kódgenerátor helyességének ellenőrzése

Jeszenszky Balázs, V. Inf., jeszyb@gmail.com

Konzulens: Dr. Majzik István, Méréstechnika és Információs Rendszerek Tanszék,
majzik@mit.bme.hu

Beágyazott rendszerek fejlesztése során egyre elterjedtebb módszerré válik a formális modelleken alapuló fejlesztés. A modelleken végrehajtott formális verifikáció segítségével sok tervezői döntés és algoritmus helyessége igazolható, így az implementáció már ellenőrzött tervek alapján indítható. Korábbi munkánk eredményeként elkészült egy olyan automatikus kódgenerátor, ami adott platformok szolgáltatásaihoz illeszkedve, könnyen paraméterezzhetően képes közvetlenül fordítható C forráskód modell alapú szintézisére. Kritikus alkalmazások esetén a generált kód felhasználásához azonban be kell látni, hogy maga a kód, valamint a kód és a futtató platform együttműködése is pontosan megfelel a modell által meghatározott viselkedésnek.

Dolgozatomban bemutatok egy olyan módszert, amivel lehetővé válik a tervezés során használt modell (időzített automaták hálózata) és a modell alapján generált alkalmazás viselkedésének összevetése, és meghatározott eltérések kimutatása. Mivel az alkalmazás komplex platformszolgáltatásokat (pl. függvénykönyvtárakat, firmware komponenseket) használhat, ezért az ellenőrzés dinamikusan történik, a modell alapján generált tesztek automatikus végrehajtásával és a teszt eredmények ellenőrzésével. A módszer és az ezt támogató keretrendszer főbb elemei a következők:

- A modell által meghatározott viselkedés ellenőrzéséhez szükséges tesztkészlet generálása automatikusan történik, kihasználva a tervezői környezet modellellenőrző komponensét. Egy olyan temporális logikai kifejezőkészletet állítok elő, aminek ellenőrzéséhez a modellellenőrzőnek el kell végeznie a modell szisztematikus bejárását (adott fedettségi kritériumok szerint), eközben absztrakt tesztesetként rögzítve a bemeneteket és az elvárt kimeneteket.
- A keretrendszer szintén automatikusan végzi az absztrakt tesztesetek leképezését olyan konkrét tesztesetekké, amelyek a vizsgált alkalmazáson (a platform interfészeihez illesztve) végrehajthatók. A megvalósítás során ugyanakkor külön ügyeltem arra, hogy fenntartsam a teszt végrehajtó komponens platformfüggetlenségét.
- A teszt végrehajtás során rögzített viselkedés (napló) és a tesztesetek által elvárt viselkedés összevetése precízen definiált reláció alapján történik. Ennek módosításával meghatározható a megengedett eltérések köre (pl. extra kimenetek elfogadása). Amennyiben a tényleges lefutás eltér a reláció szerint elvárttól, az eltérés tényén túl számos diagnosztikai kiegészítés is biztosítható.

A tesztelési folyamat során a kódgenerátort „fekete dobozként” kezeljük, tehát a megfelelő kapcsolódási pontok betartása mellett a keretrendszer más kódgenerátorral, vagy akár kézzel kódolt alkalmazás viselkedésének ellenőrzésére is alkalmazható, így a keretrendszer általánosan is támogatni tudja egy modell és egy konkrét alkalmazás viselkedése közötti eltérések tesztelését. Ehhez kiemelhető, hogy mind a modell fedettségi kritériumok, mind a teszt kiértékelési relációk módosíthatók.