



M Ű E G Y E T E M 1 7 8 2
Budapesti Műszaki és Gazdaságtudományi Egyetem
Mérés technika és Információs Rendszerek Tanszék

C programok transzformációja formális modellre



Sallai Gyula III. évf., (BSc) mérnökinformatikus szakos hallgató
Konzulensek: Hajdu Ákos doktorandusz, MIT
Tóth Tamás doktorandusz, MIT
Informatikai rendszerek szakirány, Rendszertervezés ágazat
Önálló laboratórium összefoglaló
2015/16. II. félév

Manapság mindenhol körbevesznek minket a biztonságkritikus beágyazott rendszerek: megtalálhatóak az autókban, orvosi műszerekben, vonatokon, repülőgépekben. Ahogy ezek az eszközök egyre fontosabb és nélkülözhetetlen elemeivé válnak életünknek, úgy növekszik az igény, hogy megnyugtató bizonyítékot tudjunk szolgáltatni a helyes működésükről. Az ilyen bizonyítások egy eszköze lehet a formális modellek használata. Az elkészítendő rendszer viselkedését formális modellek segítségével leírjuk, majd az épített modellen különböző lekérdezések futtatásával megtudjuk, hogy lehetséges-e egy hibás állapot. Bár ezek a módszerek képesek kielégítő bizonyítékot szolgáltatni a rendszer helyes működéséről, használatuk valós ipari projektben az idő és költségkorlátok miatt nem mindig valósul meg. Gyakori jelenség, hogy a projekt egy rövid tervezés után rögtön az implementációs fázisba ugrik, ahol legtöbbször C és/vagy Assembly nyelv segítségével valósítják meg a kívánt rendszert.

Munkám során azt vizsgáltam, hogy milyen módszerekkel lehet Assembly vagy C kódból formális modellt előállítani egy későbbi verifikáció számára. Első megközelítésben az LLVM programkönyvtár [1] egy hardverfüggetlen Assembly-hez hasonlítható nyelvét vizsgáltam ebből a szempontból, majd a végleges a projektben a C nyelvből történő transzformációt.

A transzformáció során szükség volt a C nyelvű forráskód értelmezésére, megfelelő reprezentációba történő átalakítására és a kimeneti formális modell felépítésére. Mivel a formális modell eszközkészlete korlátos, a végső transzformáció előtt szükséges a bemeneti forráskód egyszerűsítése. A cél az, hogy a későbbi műveletekhez továbbítandó bemenet a C nyelv lehető legrövidebb részhalmazát reprezentálja. A legtöbb ilyen egyszerűsítés lényege a szintaktikai kiegészítések, a különböző vezérlési szerkezetek, vagy a későbbi matematikai leírásnak nem megfogható kifejezések átalakítása. Az elkészített program kimenete a bemeneti nyelv így egyszerűsített változatának megfelelő formális modell. Ezen a modellen már a különböző verifikációs eszközök képesek hibakeresést végezni.

A félév során megvalósított program képes egy limitáltabb (**for**, **while**, **do-while**, **if-else**, **switch**, többszörös értékadás, egyoperandusú inkremens/dekremens operátorok) C nyelvű bemenet a fentieknek megfelelő egyszerűsítésére és az annak megfelelő formális modell előállítására egy tanszéki keretrendszer (TTMC) segítségével.

[1] <http://llvm.org>