

# Kritikus rendszerek absztrakcióval támogatott lineáris idejű modellellenőrzése

A technológia fejlődésével egyre több kritikus területen alkalmaznak szoftver alapú megoldásokat, ilyen esetekben azonban a szoftver hibás működése akár katasztrofális következményekhez is vezethet. Fontos feladat tehát a helyesség ellenőrzése és a hibák megtalálása lehetőleg már a fejlesztés korai fázisaiban is.

Kritikus rendszerek tervezése során gyakran használnak magas szintű modellezési nyelveket. A viselkedés leírására elterjedten használt az állapotterkép formalizmus, amely különösen alkalmas kritikus reaktív rendszerek tervezésének támogatására.

Modellek ellenőrzésére többféle megközelítés is ismert, amelyek közül a formális verifikáció alkalmas a modellek összes viselkedésének felderítésére és ellenőrzésére. Többféle formális temporális logikai nyelv is rendelkezésünkre áll a követelmények megfogalmazására, azonban kevés eszköz támogatja ezeknek a kifejező – ezáltal mérnökök által is könnyen használható – temporális logikáknak a használatát. A lineáris idejű temporális logikai specifikációk ugyan nagyon kifejezők, de ellenőrzésük különösen számításigényes feladat, emiatt az ellenőrzési módszerek hatékonyságának növelése állandó kihívás. A formális verifikáció alkalmazásának másik kihívása, hogy alacsony szintű matematikai modelleken működik, és ez megnehezíti a mérnöki alkalmazást.

Munkám célja, hogy egy olyan formális verifikációs algoritmust adjak, amely támogatja a lineáris idejű temporális logika használatát a verifikáció során. A hatékonyság érdekében egy absztrakció alapú algoritmust fejlesztettem, amely lehetővé teszi adatvezérelt reaktív rendszerek hatékony verifikációját is. Megközelítésemet egy mérnöki tervező eszközbe is integráltam, ezáltal lehetővé téve az új megközelítés mérnöki alkalmazását. Az elkészült algoritmust az egyetemen fejlesztett formális verifikációs keretrendszerben valósítottam meg, így támogatva a keretrendszer összes többi bemeneti formalizmusát is - többek között szoftverek forráskód alapú verifikációját is.

Az elkészült algoritmus hatékonyságát a szoftverellenőrzés területének egyik szabványos benchmarkján vizsgáltam meg.