Egzotikus modellellenőrzés

Önálló laboratórium feladat összefoglalója (8. félév)

Pintér Norbert (DEGA6C)
Konzulens: Bokor Péter
BME Méréstechnika és Információs Rendszerek Tanszék
Informatikai infrastruktúra tervezése szakirány, 2006/2007. II. félév

„Bounded" modellellenőrzés

Elsőként megismerkedtem a Bounded modellellenőrzési technikával. A BMC-nek rengeteg előnye van a hagyományos technikákkal szemben. A BMC sokkal gyorsabban találja meg az ellenpéldát, a megtalált ellenpélda minimális hosszúságú, valamint jóval nagyobb állapotteret képes kezelni. A BMC alapötlete, hogy a kezdeti állapotból megvizsgáljuk, hogy k lépésen belül eljuthatunk-e egy nem megengedett állapotba. Amennyiben nem, akkor k-t iteratíve növeljük egészen addig, amíg vagy találunk ellenpéldát, vagy pedig elérünk egy olyan értéket, amely esetén mondhatjuk (a vizsgált modell véges mérete miatt), hogy a rendszerünk biztonságos. Ennek a technikának van egy hatékonyabb változata, amely esetén a keresést két irányból végezzük. Egyrészt az előbb említett előrefelé haladás mellett párhuzamosan egy nem megengedett állapotból is megpróbálunk k lépésen belül elérni egy kezdeti állapotot. Ezesetben azonban problémák merülnek fel a visszafelé haladást illetően, létrejönnek úgynevezett „hamis" ellenpéldák, hiszen visszafelé nem megengedett átmeneteken haladhatunk. Természetesen ezen probléma kezelésére is van megoldás, mégpedig lemmák bevezetésével, melyekkel definiálni tudom a visszafelé haladást. Ez a technika azonban csak invariánsok modellellenőrzésére használható.

Végtelen állapotterű modellek modellellenőrzése

Ezután behatóbban tanulmányoztam a SAL model checker eszközt, illetve megismerkedtem a működésével. A SAL eszköz megismerkedése közben tanulmányoztam a timed-automata és egyéb automata modelleket és azok lehetséges implementálását, illetve vizsgálatát a sal-inf-bmc segítségével, amely a SAL-nak az infinite modellek vizsgálatához kifejlesztett eszköze. A fent említett modell tipikusan végtelen állapotterű modell. Ez az eszköz egyrészt tartalmaz egy absztrakciós technikát amely az úgynevezett időintervallumokon alapul és képes bizonyos modellek (tipikusan a timed-automaták) esetén a végtelen állapotú modellt véges állapotterűvé alakítására úgy, hogy az időt diszkretizálja. Ennek köszönhetően ezen modellek vizsgálata már jóval egyszerűbbé válik és a hagyományos BMC technikákkal vizsgálható, illetve a k-indukciós technikával pedig bizonyíthatóvá válik a modellek helyessége. Azonban mint kiderült a végtelen modellellenőrzés nem általános technika, nem tudunk tetszőleges végtelen modelleket modellellenőrizni!

Biztonsági protokollok

A félév végén pedig elkezdtem megvizsgálni a modellellenőrzés lehetséges alkalmazásait a biztonsági protokollok területén. Megvizsgáltam, hogy ezen területen mely tényezők okozzák az állapottér robbanását. Megismerkedtem az AVISPA eszközzel, megvizsgáltam benne néhány egyszerűbb protokoll ellenőrzését. Végezetül pedig elkezdtem megvizsgálni az eszköz által használt absztrakciós technikákat. Rájöttem, hogy a résztvevők, illetve a session-ök száma még mindig nagy problémát okoz a protokollok modellellenőrzésében. További céljaim, hogy a már létező technikákat egy általánosabb kontextusba helyezzem, illetve meg szeretném vizsgálni, hogy esetleg milyen új absztrakciós technikát lehetne alkalmazni.