Múlt és jövő: Új algoritmusok lineáris temporális tulajdonságok szaturáció-alapú modellellenőrzésre

A technológia fejlődésével a számítógépes rendszerek alkalmazási köre ma már olyan biztonságkritikus rendszerekre is kiterjed, amelyek helyes működésétől sokszor teljes vállalatok sorsa, vagy akár emberéletek is függhetnek. Az ilyen rendszerek mérete és bonyolultsága ráadásul egyre nő, így szükség van megbízható, automatikus ellenőrző módszerek kifejlesztésére. A formális módszerek a tervezési folyamat helyességét garantálják azzal, hogy matematikai igényességgel igazolják a rendszer (biztonság szempontjából) kritikus tulajdonságainak teljesülését.

A biztonságkritikus rendszerek formális verifikációjára az elmúlt évtizedekben számos módszert dolgoztak ki, és a terület ma is dinamikusan fejlődik. Az egyik ilyen módszer a modellellenőrzés, amely a rendszerekről készített modellek lehetséges állapotait veszi számításba és veti össze a formalizált követelményekkel, hibás állapotszekvenciákat keresve. Az ún. szaturációs algoritmus egy új, rendkívül hatékony megközelítés nagyméretű, párhuzamos és aszinkron rendszerek állapotainak szimbolikus felderítésére. Kutatásaink során elsőként javasoltunk szaturáció alapú algoritmust lineáris idejű temporális logikával (LTL) leírt tulajdonságok modellellenőrzésére. Akkori megoldásunk újszerűsége mellett azonban nem volt kellően általános megközelítés, ez pedig gátat szabott az ellenőrizhető rendszerek bonyolultságának.

Jelen dolgozatban a lineáris idejű modellellenőrzőnk számos továbbfejlesztését és kiterjesztését mutatjuk be. Új eredményeink közül a legfontosabbnak az ún. múlt idejű lineáris temporális logikával (PLTL) leírt specifikációk támogatását tartjuk. Jelentősen optimalizáltuk, javítottuk a modellellenőrzés köztes lépéseit is, és az egyes részproblémákra új, a korábbi módszereknél hatékonyabb és egyszersmind általánosabb algoritmust adtunk. A használt modellek tekintetében a korábban csak színezetlen Petri-hálókon működő modellellenőrzőt képessé tettük közvetlenül színezett Petri-hálókon való működésre is, így jelentősen bővítve az ellenőrizhető modellek körét. Munkánk legjobb tudomásunk szerint egyedülálló, mivel rajtunk kívül korábban semmilyen olyan, általunk ismert megoldást nem publikáltak a lineáris idejű modellellenőrzés problémájára, ami a rendkívül hatékony szaturációs algoritmust és a PLTL formalizmust használta volna.