

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

A technológia fejlődésével a digitális technika 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 csak nő, így szükség van megbízható, automatikus ellenőrző módszerek kifejlesztésére. A tervezési folyamat biztonságossá tételére formális módszerek használhatók, matematikai igényességgel garantálva a helyes működést.

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 állapotokat keresve. Az ún. szaturációs algoritmus egy új, rendkívül hatékony megközelítés nagyméretű, párhuzamos és aszinkron rendszerek állapotainak szimbolikus felderítésére. Korábbi kutatásaink során sikerrel alkalmaztuk az algoritmust lineáris idejű temporális logikát (LTL) használva, új megoldásokat javasolva a CTL-alapú modellellenőrzéstől eltérő algoritmikus kihívásokra.

Jelen dolgozatban a lineáris idejű modellellenőrzőnk számos továbbfejlesztését és kiterjesztését mutatjuk be. Új eredményeink közül a legfontosabbak közé tartozik az ún. múltidejű lineáris temporális logika (PLTL) bevezetése. Jelentősen optimalizáltuk, javítottuk a modellellenőrzés köztes lépéseit is, és az egyes részproblémákra új, a korábbi módszereknél hatékonyabb és egyszersmind általánosabb algoritmust is adtunk. A használt modellek tekintetében a korábban csak színezetlen Petri-hálókon működő modellellenőrzőt képessé tettük közvetlenül színezett Petri-hálókon való működésre is. 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.

Past and future: Novel algorithms for saturation-based model checking of linear temporal properties

With the evolution of computer technology, we can witness an increasing involvement of digital techniques in safety-critical domains. These applications must be highly reliable, since in many cases, whole companies or even human lives depend on their correct behaviour. To handle the ever-increasing complexity of these systems, we need to develop creditable, automatic verification techniques. To ensure the correctness of the design process, one can use formal methods to mathematically prove the critical properties of the system under development.

In the last decades, many methods have been developed for the formal verification of safety-critical systems, and the domain is still evolving dynamically. One of these is model checking, a method that computes the states of the system model, checking them against its formal requirements looking for violating states. The saturation algorithm is a relatively new approach to the symbolic state space exploration of large, parallel and asynchronous systems that proved to be very efficient. In our previous research, we successfully utilized this algorithm for model checking linear temporal properties (LTL), proposing novel solutions to the different challenges that LTL presents compared to CTL model checking.

In this work, we introduce the numerous improvements and extensions we made to our linear-time model checker. One of our most important new results is the introduction of past-time linear temporal logics (PLTL). We also improved and optimized the intermediate steps of the model checking process, developing more efficient and general algorithms for the individual subproblems. In the terms of supported model formalisms, beside uncoloured Petri nets, we now support direct verification of coloured Petri nets as well. To the best of our knowledge, our work is unique, since we do not know about any published linear temporal model checking approaches that use the remarkably efficient saturation algorithm together with the usage of PLTL notation.