ADVANCED SATURATION-BASED MODEL CHECKING

Vince Molnár, XD5Z68

Abstract

Efficient symbolic and explicit model checking approaches have been developed for the verification of linear time temporal logic (LTL) properties. Nowadays, several attempts have been made to combine on-the-fly search with symbolic encoding. Model checking LTL properties usually pose two challenges: one must compute the product between the state space of the system and the automaton model of the desired property, then look for counterexamples that is reduced to searching for fair loops or strongly connected components (SCCs) in state space of the product. In case of concurrent systems, the so-called saturation algorithm proved to be an efficient symbolic state space generation approach.

This thesis proposes a new approach that leverages the saturation algorithm both as an iteration strategy used to compute the product directly, as well as in a new incremental fixed-point computation algorithm to compute strongly connected components on-the-fly. Complementing the search for SCCs, explicit techniques and abstraction will be used to prove the absence of counterexamples. The result is an on-the-fly, incremental LTL model checking algorithm that proved to scale well with the size of models, as evaluation on models of the Model Checking Contest suggests.

SZATURÁCIÓ ALAPÚ MODELLELLENŐRZÉS KITERJESZTÉSÉNEK VIZSGÁLATA

Molnár Vince, XD5Z68

Kivonat

A lineáris temporális logikai (LTL) specifikációk verifikációjára számos explicit és szimbolikus modellellenőrzési technikát dolgoztak ki az elmúlt évtizedekben. Manapság a kutatások meghatározó iránya a két algoritmuscsalád előnyeinek kombinálása, legfőképp az ún. "on-the-fly" (menet közbeni) modellellenőrzés megvalósítása szimbolikus kódolást használva. Az LTL modellellenőrzés megvalósításához két problémát kell megoldani: ki kell számolni a rendszer állapotterének és a követelményt leíró automatának a szinkron szorzatát, majd ebben ellenpéldákat, vagyis hibás lefutásokat keresni. Utóbbi visszavezethető körök vagy erősen összefüggő komponensek keresésére a szorzatot leíró gráfban. Konkurens rendszerek esetén az ún. szaturációs algoritmus nagyon hatékony megoldásnak bizonyult a szimbolikus állapottér-felderítés problémájának megoldására.

Jelen diplomamunka célja egy olyan új megoldás bemutatása, amely a szaturációs algoritmus előnyeit mind a szorzat közvetlen kiszámításában, mind egy erősen összefüggő komponenseket kereső inkrementális fixpont-számító algoritmusban kiaknázza. A keresést kiegészítve explicit megoldások és absztrakció segítségével a bemutatott algoritmus menet közben az ellenpélda hiányát is megpróbálja bebizonyítani. Az eredmény egy "on-the-fly" működésű, inkrementális LTL modellellenőrző algoritmus ami a Model Checking Contest modelljein végzett kísérletek alapján jól skálázódik a vizsgálandó modell méretével.