Title	分割統治による誘導性と条件付安定性のモデル検査
Author(s)	YATI, PHYO
Citation	
Issue Date	2022-09
Type	Thesis or Dissertation
Text version	ETD
URL	http://hdl.handle.net/10119/18134
Rights	
Description	Supervisor:緒方 和博, 先端科学技術研究科, 博士

A Divide & Conquer Approach to Leads-to and Conditional Stable Model Checking

Yati Phyo

September, 2022

Abstract

Model checking is one of the most successful computer science achievements in the last few decades. This is why Edmund M. Clarke, E. Allen Emerson and Joseph Sifakis were honored with 2007 A.M. Turing Award for their role in developing model checking into a highly effective verification technology. Model checking has been widely adopted in industries, especially in hardware ones. There are still some. issues to tackle in model checking, one of which is the notorious state explosion. Many techniques to mitigate the state explosion, such as partial order reduction and abstraction, have been devised. Because these existing techniques are not too enough to deal with the state explosion, however, it is still worth tackling it.

To mitigate the state space explosion problem to some extent, we propose a divide & conquer approach to model checking (DCA2MC) leads-to properties and conditional stable properties, where leads-to properties are expressed in $\varphi_1 \leadsto \varphi_2$ and conditional stable properties are expressed in $\varphi_1 \leadsto \Box\varphi_2$, where φ_1 and φ_2 are state propositions or classical propositional formulas. Chandy and Misra designed a temporal logic called UNITY in which the leads-to temporal connective plays an important role and demonstrated that many important systems requirements can be expressed as leads-to properties. Moreover, Dwyer et al. showed some statistics on the usage distribution of the various patterns in property specifications in which the leads-to property (or the response pattern) had the highest proportion. Conditional stable properties can be used to express core requirements in self-stabilizing systems, which were first introduced by Dijkstra and became a very important concept in fault tolerance to design robust systems. Thus, it is worth focusing on leads-to and conditional stable properties. DCA2MC divides an original leads-to (or conditional stable) model checking problem into multiple smaller model checking problems and tackles each smaller one. We prove a theorem that the multiple smaller model checking problems are equivalent to the original leads-to (or conditional stable) model checking problem. An algorithm is constructed based on the theorem to support model checking leads-to (or conditional stable) properties by DCA2MC. A support tool is developed in Maude, a rewriting logic-based specification/programming language and system, to support the technique based on the algorithm for each of leads-to and conditional stable properties. Some experiments are then conducted with the support tools to demonstrate that our tools/techniques can mitigate the state space explosion to some extent.

Both leads-to and conditional stable properties can be expressed as linear temporal logic (LTL) formulas that are very similar. However, how to deal with the two classes of properties with DCA2MC is so different that we need to prove the correctness of DCA2MC for the two classes of properties in two different ways and come up with two different algorithms for the two classes of properties, from which the two support tools are built. Note that because the architecture of the tools is well-designed, many components (data structures and functions) are shared by the two tools. This is because it suffices to take a look at the top state of an infinite sequence π of states so as to check if a state proposition φ_2 holds for π, while it is necessary to take a look at all states in π in order to check if an LTL formula $\Box\varphi_2$, where φ_2 is a state proposition, holds for π. One piece of our future work is to extend DCA2MC for the other classes of LTL properties and then come up with a unified DCA2MC for all LTL properties.

Keywords: LTL model checking, leads-to properties, conditional stable properties, state space explosion, divide & conquer.