Compositional Verification and 3-Valued Abstractions Join Forces

Orna Grumberg

Computer Science Department, Technion, Haifa, Israel

Abstract

Model checking is a useful approach for verifying properties of systems. It is given a model M of a system and a temporal logic formula φ, describing a specification. It returns 'true' if the system satisfies the specification ($M \models \varphi$) and 'false', otherwise. The main disadvantage of model checking is the state explosion problem, which refers to its high space requirements.

Two of the most promising approaches to fighting the state explosion problem are *abstraction* and *compositional verification*. In this work we join their forces to obtain a fully automatic compositional technique that can determine the truth value of the full μ-calculus with respect to a given system.

In the talk we first briefly explain what model checking is. We then present the needed background on abstraction and on compositional verification. Next we describe our approach in more detail.

Given a system $M = M_1 \| M_2$, we view each component M_i as an abstraction $M_i\uparrow$ of the system M. The abstract component $M_i\uparrow$ is defined using a 3-valued semantics so that whenever a formula φ has a definite value (true or false) on $M_i\uparrow$, the same value holds also for M. Thus, φ can be checked on either $M_1\uparrow$ or $M_2\uparrow$ (or both), and if any of them returns a definite result, then this result holds also for M.

If both checks result in an indefinite value, the composition of the components needs to be considered. However, we would like to avoid the full composition of $M_1\uparrow$ and $M_2\uparrow$. Instead, our approach identifies and composes only the parts of the components in which their composition is necessary for concluding the truth value of φ. It ignores the parts which can be handled separately. The resulting model is often significantly smaller than the full system.

We explain how our compositional approach can be combined with abstraction, in order to further reduce the size of the checked components. The result is an incremental compositional abstraction-refinement framework, which resembles automatic Assume-Guarantee reasoning.

This is a joint work with Sharon Shoham.