3-Valued Abstraction-Refinement

Orna Grumberg
TECHNION, Haifa, Israel

Model checking is a technique that given a model of a system and a specification written in a temporal logic, determines whether the system model satisfies the specification. Model checking is widely used for hardware and software verification. Its main limitation, however, is due to its high memory requirements, referred to as the *state explosion problem*.

One of the most successful approaches to fighting the state explosion problem is *abstraction*. With this approach, a small abstract model of the system is constructed, by hiding some of the system details that are not relevant to the checked property.

Typically, abstractions are conservative with respect to "true" results. That is, if the property is true of the abstract model then it is also true of the concrete full model. However, if the property is false in the abstract model then nothing can be concluded of the concrete model. In this case the abstract model should be refined, thus making it "closer" to the concrete one. This type of abstractions usually handle only the universal fragments of temporal logics and are based on a 2-valued semantics.

A different approach to abstraction-refinement uses a 3-valued semantics in which a property can be evaluated on the abstract model to "true", "false", or "unknown". The abstract model is constructed in such a way that if a property is either "true" or "false" in the abstract model then it is "true" or "false" respectively in the concrete model as well. Only in cases the value of the property in "unknown" that a refinement is needed. 3-valued abstractions are powerful since they can be used for both verification and refutation of properties. Further, they can handle full branching temporal logic (e.g. CTL, CTL*, μ-calculus) and not just their universal fragment.

In these talks we will present 3-valued abstraction and refinement. We will consider several of its applications, including compositional model checking and hardware verification.

References

1. O. Grumberg. *Abstraction and Refinement in Model Checking*. Proc. "International Conference on Formal Methods for Components and Objects" (FMCO 2005), LNCS 4111, 2005.