

Hierarchical reasoning and quantifier elimination for the verification of parametric reactive and hybrid systems

Viorica Sofronie-Stokkermans

University Koblenz-Landau and Max-Planck-Institut für Informatik, Saarbrücken

Abstract

Most of the applications in verification require reasoning about complex domains. In this paper we identify several classes of verification problems for parametric reactive systems (modeled by transition constraints) and for certain classes of hybrid systems, and point out the reasoning tasks in the associated theories which need to be solved. The type of parametricity we consider refers to parametric data (including parametric change and environment) specified using functions with certain properties and parametric topology, specified using data structures.

- The first problem we address is to check whether a safety property – expressed by a suitable formula – is an invariant, or holds for paths of bounded length, *for given instances of the parameters*, or *under given constraints on parameters*. For this type of problems, we aim at identifying situations in which decision procedures exist.
- We also analyze the dual problem – related to system synthesis – of *deriving constraints between parameters* which guarantee that a certain safety property is an invariant of the system or holds for paths of bounded length.
- Finally, we study possibilities of automatically generating criticality functions (used in the analysis of hybrid systems to characterize regions where safety properties can be guaranteed).

We identify properties of the underlying theories which ensure that these classes of verification problems can be solved efficiently. In particular, we present possibilities of using hierarchical reasoning, quantifier elimination and model generation for the verification of parametric systems. We illustrate our methods on several examples.