Universität Basel

Publication

Abstraction-based guided search for hybrid systems

ConferencePaper (Artikel, die in Tagungsbänden erschienen sind)

Hybrid systems represent an important and powerful formalism for modeling real-world applications such as embedded systems. A verification tool like SpaceEx is based on the exploration of a symbolic search space (the region space). As a verification tool, it is typically optimized towards proving the absence of errors. In some settings, e.g., when the verification tool is employed in a feedback-directed design cycle, one would like to have the option to call a version that is optimized towards finding an error path in the region space. A recent approach in this direction is based on guided search. Guided search relies on a cost function that indicates which states are promising to be explored, and preferably explores more promising states first. In this paper, an abstraction-based cost function based on pattern databases for guiding the reachability analysis is proposed. For this purpose, a suitable abstraction technique that exploits the flexible granularity of modern reachability analysis algorithms is introduced. The new cost function is an effective extension of pattern database approaches that have been successfully applied in other areas. The approach has been implemented in the SpaceEx model checker. The evaluation shows its practical potential.