State-space reduction for probabilistic model checking

Description

Model-checking is a popular verification technique aiming at automatically the satisfaction of a given property by an input model. The basic approach to model-checking involves an exhaustive exploration of the model state-space looking for violations of the property. If a violation is found, it is reported to the user, possibly accompanied with a counter-example showing how to reproduce it. Probabilistic model-checking is concerned with the verification of quantitative properties of probabilistic models. An example of such properties is "the probability of kernel meltdown for a nuclear plant has to be lower than $10^{-7}$" or "the probability of an airplane to fall down has to be lower than $10^{-5}$". Besides providing a suitable framework for describing uncertainty in model assumptions, probabilistic models come into play for the description of many physical phenomena the system has to interact with. A critical problem with exhaustive search is the combinatorial exposition of the state space to be explored. Even simple systems may require a large number of states to be properly represented. State-space reduction techniques aim at reducing the number of states to be explored, allowing for quite large models to be analyzed. Different techniques provide better results depending on specific characteristics of the models under analysis.

The goal of this seminar is to compare different state-space reduction techniques for probabilistic model-checking in order to report their strengths and pitfalls and to guide the engineers in choosing the most effective for his case. The focus of the seminar is on three techniques for the probabilistic model-checking of finite states time homogeneous Markov processes.

This work might be optionally extended for a MS Thesis.

Prerequisites

A basic knowledge of SAT and SMT, and familiarity with automata and logics are required.

References


Contacts

Antonio Filieri (filieri@informatik.uni-stuttgart.de)
Reliable Software Systems (RSS) Group
Institute for Software Technology (ISTE)
University of Stuttgart