Model Checking Abstract State Machines with [mc]square

Motivation

Abstract State Machines (ASM) are a formal method for designing and analysing systems with a high level of abstraction. The goal of this diploma thesis is embedding the open-source-Simulators CoreASM into [mc]square. This requires the serialization of the simulator's states and the determination of non-deterministic characteristics such as scheduling the simulator. It is crucial to ensure the compatibility to future versions of CoreASM.

Task

Our model-checking tool [mc]square is currently used to verify assembler source code for specific microcontrollers (e.g. ATMEL ATmega16 und Infineon XC 167). The approach being used can also be transferred to ASMs very well due to the tool's architecture. Your task is to present to what extent optimizations that are used for verifying assembler programs are applicable.

Required Knowledge

You must have good skills in Java for the implementation that is required in the scope of this thesis.

Tutor

- Dr.-Ing. Daniel Klünder