

Masterthesis

A Conformance Relation for Symbolic Timed Automata with continuous Variables

Topic

The COMPASS-tool allows model-checking for formal system specifications. These specifications are written in AADL, a language used for model-based software development. The COMPASS-tool has successfully been applied in the development process of the European Space Agency (ESA), checking large models that describe i.e. the behaviour of satellites. Even though some errors can be found in the early modelling phase, the final implementation has to be tested if it conforms to its formal specification. This testing process is crucial for the software reliability, consumes a lot of time and requires at least 30-40% of the total software developing cost.

One promising method to automate the test process, and therefore reduce time and cost, is model-based testing. Model-based testing is a so called black box testing, which automatically derives the test-cases from a formal specification describing the desired behaviour of the implementation under test (IUT). These test-cases are then executed against the real IUT by stimulating the implementation and observing its output. One framework for model-based testing is the stioco framework, where the specification is given as a timed automata with variables that are passed through input and output actions. The conformance relation, called stioco, describes that an implementation may only produce outputs or be silent if the same outputs or silence are also produced by its specification.

In order to apply model-based testing on AADL models a translation to transition systems has been developed. The resulting transition system is a symbolic timed automata with continuous variables. The continuous variables are due to the originated AADL model and so far there is no model-based testing theory which allows the use of this kind of automata.

Task

In order to do model-based testing a formal correctness criteria, a so called conformance relation, is needed. Such a relation already exists for symbolic timed automata, called stioco, but not for symbolic timed automata with continuous variables. The aim of this thesis is to define such a conformance relation based on previous relations and show its correctness.

Requirements

You should be interested in formal methods and ideally have attended lectures from the Chairs I2 or I7.

Contact

If you are interested please contact Sabrina von Styp, i2, E1 4205, (von-styp@cs.rwth-aachen.de).