Static Analysis of Microcontroller Software using SAT- and Constraint-Solving

Motivation

Classical static analysis problems such as reaching definitions analysis or live variables analysis can not only be described by means of equation system, but it is also well-known that such analyses can equivalently be defined as set-constraints [Aik99]. Recently, there have been manifold advances in Boolean satisfiability solvers, making it possible to analyze formulae consisting of millions of variables.

Task

The aim of this thesis is to utilize recent advances in the field of SAT/SMT and constraint solving in order to implement scalable static analyses. These techniques shall be integrated into [mc]square, which is a model checker for microcontroller assembly code. Apart from deriving encodings of classical analyses, the student shall develop and implement methods for performing value-set analysis of microcontroller assembly code.

Fields of Study

- Computer science

Required Knowledge

- Java
- Basic knowledge of embedded systems and microcontroller programming

Student

- Lucas Brutschy

Tutor

- Dr. rer. nat. Jörg Brauer