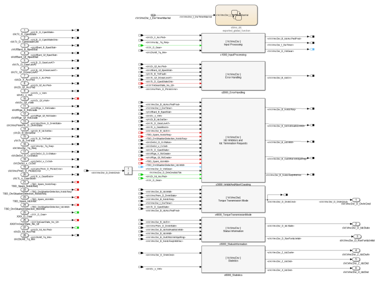
Software Modeling
and Verification Chair

RWTH AACHEN
UNIVERSITY

— Master's Thesis —

Formal Verification of Industrial C Code

What is it all about? Formal Verification of industrial code is in its infancy and, while academic tools perform well on some specific examples, most can not handle a general setting that combines next-to all aspects of the C language in a real-word setting. With this master thesis we want to investigate the current state-of-the-art in academic model checking of C code that is automatically generated from Simulink open-loop controller models. You will look at the Software Verification competition (SVcomp) for comparison and then apply a few academic model checkers like Ultimate an SMACK to two challenging Ford R&D prototype case studies: a next-gen Driveline State Request and a next-gen E-Clutch Control. The DSR feature takes driver interactions and vehicle status information to decide in which situations the driveline[1] should be opened and closed again. The ECC feature calculates the desired clutch torque capacity and corresponding engine control torques or speeds for opening and closing the driveline.



These case studies contain various features (decision logic, floating-point arithmetic, rate limiters and state-flow systems) implemented in discrete-time logic. The diverse features and the extensive use of floating-point variables make the formal code verification highly challenging. Most academic tools implement a wide variety of optimizations and heuristics, but the user is responsible for selecting the right combination. You will cooperate with tool developers in mapping available features, their applicability and impact as well as opportunities for adding new optimizations yourself.

What is to be done?

You will

1. assess the current state of the art in formal verification of C code and select one to three academic tools,
2. apply the selected tools on two case studies provided by Ford, our partner in this project and
3. compare the tools in usability and performance as well as identify and work on possible shortcomings and missing key features.

Requirements

- Enthusiasm!
- A solid background in theoretical computer science.
- Lectures on model checking and logic.

Contact

- Philipp Berger, berger@cs.rwth-aachen.de, Tel. 0241/80-21206.

[1] A motor vehicle's driveline consists of the parts of the powertrain excluding the engine. It is the portion of a vehicle, after the prime mover, that changes depending on whether a vehicle is front-wheel, rear-wheel, or four-wheel drive.