Karlsruher Institut für Technologie

Institut für Theoretische Informatik (ITI)
Anwendungsorientierte Formale Verifikation
Prof. Dr. Bernhard Beckert

Masterarbeit – Praxis der Forschung

Property-Directed Reachability for Regression Verification

Background. Since 2007, IC3 and property-directed reachability (PDR) became de-facto standard in the domain of symbolic model checking. Both approaches are decision procedures to verify that a given invariant holds for the modelled system.

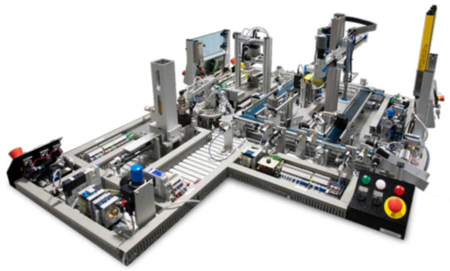
With Regression Verification, we can prove that two given systems with the same behaviour are functionally equivalent (minus the intended changes). In our case we apply Regression Verification in the field of automated production systems to ensure the well-functioning during software evolution.

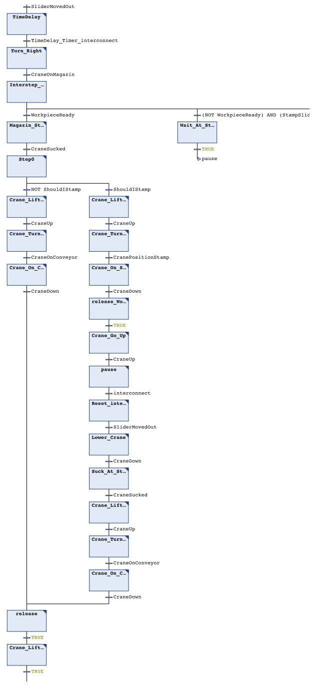
Goal. The goal of this thesis is the transfer of current PDR/IC3 approaches to software model checking in order to outperform current regression verification implementations. The idea is to exploit the main assumption behind regression verification, which is that both software versions have a high degree of similar structures. As a benchmark scenario we use the Pick-and-Place-Unit from TUM.

Task. Your task is to understand the current State-of-the-Art of PDR and IC3; adapt the ideas into a novel approach, and perform the benchmarks.

Your profile. Programming skills on C/C++ and Java required. Furthermore, you should be interested in programming languages and SAT solving. You should have completed the Formal Methods (Formale Systeme) Course at KIT or equivalent.

References. **(1)** Aaron R. Bradley. SAT-based Model Checking Without Unrolling. VMCAI 2011. **(2)** Alessandro Cimatti and Alberto Griggio. Software model Checking via IC3. CAV 2012. **(3)** Tim Lange, Martin R. Neuhäußer, and Thomas Noll. IC3 Software Model checking on control flow automata. FMCAD 2015.





Kontakt

Alexander Weigl weigl@kit.edu Office: 50.34, R225