

Masterarbeit – Praxis der Forschung

Maschinelles Lernen von Invarianten für die Regression Verifikation

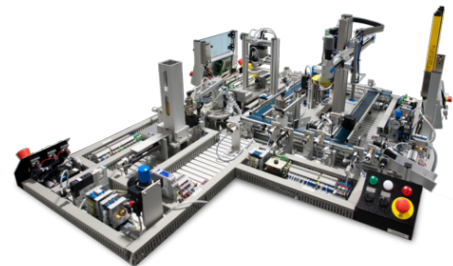
Hintergrund. Seit 2007 wurden *IC3* und *Property-Directed Reachability (PDR)* zum Platzhirschen im Bereich der symbolischen Modellprüfung (*Model-Checking*) von Invarianten. Beide Entscheidungsprozeduren verifizieren, ob eine Invariante in jedem erreichbaren Zustand eines Systems gilt. Dazu lernen diese aus dem System und der spezifizierten Invariante eine neue, stärkere und induktive Invariante.

Regression Verifikation (RV) ist eine Erweiterung der Äquivalenzprüfung zweier Systeme. Mit RV können wir sicherstellen, dass zwei Systeme sich in ihrem Verhalten nicht unterscheiden, abgesehen von gewünschten Änderungen, z. B. Bug fixes oder Optimierungen. Wir wenden RV im Bereich von automatisierten Produktionssystemen an, um eine korrekte Funktionalität über die Softwareevolution sicherzustellen.

Ziel. Das Ziel dieser Arbeit ist der Transfer von aktuellen *IC3* und *PDR* Ansätzen auf die Regression Verifikation um die schneller zu sein als der naive Ansatz über Produktprogramme. Die Idee dabei ist die Ausnutzung einer der Hauptannahmen hinter Regression Verifikation: Beide Softwareversionen sind zu einem hohen Grad strukturell identisch. Als Benchmark dienen die Szenarien der Pick-and-Place-Unit von der TU München.

Dein Profil. Programmkennnisse in C/C++ und Java/Kotlin erforderlich. Weiterhin solltest du ein Interesse an Programmiersprachen und SAT-Solving mitbringen. Du solltest die Veranstaltung *Formale Systeme* am KIT oder Vergleichbares erfolgreich abgeschlossen haben.

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. Neuhäuser, and Thomas Noll. IC3 Software Model checking on control flow automata. FMCAD 2015.



Kontakt

Alexander Weigl

weigl@kit.edu

Office: 50.34, R225