Karlsruher Institut für Technologie

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

Ermittlung von Zuverlässigkeitsmaßen durch Bounded Model Checking

Praxis der Forschung SS 2021

Hintergrund

Bounded Model Checking ist eine Technik, bei der die Korrektheit eines Programms für Programmausführungen beschränkter Länge gezeigt wird, indem z.B. Schleifen ausgerollt werden. Die Länge der Ausführungspfade, die überprüft werden, kann erhöht werden, bis ein Fehler gefunden wird oder der Beweisprozess zu lange braucht.

Es existieren Verfahren, mit denen man aus unvollständigen Beweisen wie denen, die BMC erbringt, bestimmen oder abschätzen kann, für wie viele mögliche Eingaben das Programm sich korrekt verhält. Bei ereignis- und sensorgesteuerten Prozessen wie Ampelschaltungen oder Steuerungssoftware ergibt es allerdings nicht wirklich Sinn, von einer konkreten Eingabe zu sprechen, da das Programm immer wieder auf neue Eingaben reagiert, die es teilweise selbst beeinflusst. Stattdessen wüsste man gerne, wie viele Fehler im Durchschnitt in einer bestimmten Zeitspanne passieren oder wie oft der Prozess im Durchschnitt abstürzt.

Aufgabe

Das Ziel dieses Projektes ist, mit Hilfe formaler Verifikation die Zuverlässigkeit von Programmen zu bestimmen.

Ihre Aufgabe ist es, Bounded Model Checking zu verwenden, um die Zuverlässigkeit eines Programms zu verifizieren. Sie sollen ein Verfahren entwickeln, das es erlaubt, aus unvollständigen Korrektheitsbeweisen bestimmte Zuverlässigkeitsmaße (Ausfallwahrscheinlichkeit, *Mean time to failure*) zu extrahieren oder abzuschätzen.

Literatur

- Belli, F., Grochtmann, M. & Jack, O.: Erprobte Modelle zur Quantifizierung der Software-Zuverlässigkeit. *Informatik-Spektrum Vol. 21*, S. 131–140 (1998). `https://doi.org/10.1007/s002870050094`
- Biere, A., Cimatti, A., Clarke, E., Strichman, O., Zhu, Y.: Bounded Model Checking. *Advances in Computers Vol. 58*, S. 117-148 (2003). `https://doi.org/10.1016/S0065-2458(03)58003-2`
- Clarke, E., Kroening, D., Lerda, F.: A Tool for Checking ANSI-C Programs. *10th International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, S. 168-176 (2004). `https://doi.org/10.1007/978-3-540-24730-2_15`

Ansprechpartner

- Dr. Mattias Ulbrich, ulbrich@kit.edu, Büro 50.34R229
- Florian Lanzinger, lanzinger@kit.edu, Büro 50.34R203