ICT15-103 - APALACHE: Abstraction-based Parameterized TLA Checker

Zusammenfassung

Moderne Internetdienste, wie die von Amazon, Google, Facebook, oder Netflix, laufen in der Cloud. Benutzeranfragen werden von zehntausenden Computern bearbeitet, die sich in weltweit verteilten Datenzentren befinden. Bei so vielen involvierten Computern werden Fehler von der Ausnahme zur Regel. Gleichzeitig verspricht in den letzten Jahren die neue Blockchaintechnologie das Entstehen offener, kryptographischer, konsensbasierter Wirtschaftsnetzwerke. Der dezentrale Charakter dieser Netzwerke, bestehend aus tausenden Computern, verspricht robustere globale Wirtschaftssysteme mit gerechteren und demokratischeren Möglichkeiten für alle. Dieses Versprechen kann aber nur eingelöst werden, wenn die Blockchainsysteme tatsächlich fehlertolerant sind und nicht von einzelnen Angreifern kompromitiert werden können. Daher wird es immer wichtiger Fehlertoleranzmechanismen auf rigorose Art zu entwerfen und zu verifizieren, dass diese Mechanismen tatsächlich ihre Aufgaben erfüllen.

TLA+ ist ein Formalismus, den Turing-Preisträger Leslie Lamport erfunden hat, um solche Fehlertoleranzmechanismen zu entwerfen. Das APALACHE Projekt widmete sich automatischen Verifikationsmethoden für TLA+. Wir entwickelten ein Model-Checking-Programm namens Apalache, das modernste automatische Verifikationsmethoden auf TLA+ anwendet. Mittels Apalache können heute Fehlertoleranzmechanismen für kleine Systeme verifiziert werden. Im Vergleich mit dem von Microsoft Research gepflegten TLC Model Checker, gibt es bereits jetzt viele Anwendungen bei denen Apalache effektiver arbeitet. Wir befinden uns im regelmäßigen Austausch mit Leslie Lamport und den TLA+ Arbeitsgruppen von Microsoft Research und Inria Nancy, und sind gerade dabei die Einbindung von Apalache in die TLA+ Toolbox vorzubereiten. Dieses von Microsoft gepflegte Programm wird weltweit zum Entwurf verteilter Systeme verwendet. Der typische Ansatz zur Sicherstellung der Korrektheit von Spezifikation für Tausende von Computern besteht in TLA+ aus zwei Schritten: (1) Ausführen von TLC und Apalache, um die Spezifikation für eine kleine Anzahl von Teilnehmern zu debuggen, und (2) Formalisieren des Korrektheitsbeweises für eine beliebige Anzahl von Teilnehmern mit dem interaktiven Theorembeweiser TLAPS. Bei realistischen Systemen umfasst dies in der Regel mehrere Personenmonate Arbeit von Verifizierungsingenieurinnen. Ein vollautomatischer Ansatz für (2) wird als parametrisiertes Model Checking bezeichnet. Es stößt an viele theoretische und praktische Grenzen.

Wir haben neue parametrisierte Verifikationsmethoden für fehlertolerante Algorithmen entwickelt und diese neuen Methoden in unserem Tool ByMC (Byzantine Model Checker) implementiert. Unser nächstes Ziel ist es, Apalache und ByMC zu verbinden. Die Arbeit des Apalacheprojektes findet international große Anerkennung. Von wissenschaftlicher Seite haben wir bereits im Jahr 2020 mehrere Einladungen für Vorlesungen und Tutorials in die USA, Belgien, und Malta. Von industrieller Seite wurden die beiden Projektleiter Igor Konnov und Josef Widder von Informal Systems Inc. angestellt, um an der Verifikation der Tendermint Blockchain zu arbeiten sowie den Apalache Model Checker weiterzuentwickeln. Daraus resultierte die Gründung einer österreichischen Tochterfirma, der Informal Systems GmbH mit Sitz in Wien, und der Schaffung von zurzeit vier höchstqualifizierten Arbeitsplätzen in Wien.

Wissenschaftliche Disziplinen:
Software development (50%) | Distributed systems (40%) | Mathematical logic (10%)

Keywords:
computer-aided verification, model checking, parameterized verification,TLA+, fault-tolerant distributed algorithms

Principal Investigator: Igor Konnov

Institution: Vienna University of Technology

Co-Principal Investigator(s): Josef Widder (Vienna University of Technology)

Status: Abgeschlossen (01.01.2016 - 31.12.2019)

Weiterführende Links zu den beteiligten Personen und zum Projekt finden Sie unter
https://www.wwtf.at/funding/programmes/ict/ICT15-103/