ICT19-060 - Learning to Solve Quantified Boolean Formulas

Zusammenfassung

Fehler in Hard- und Software können teuer sein und zu drastischen Konsequenzen in kritischer Infrastruktur führen. Der Bereich der "formalen Methoden" beschäftigt sich damit, nachzuweisen, dass Hard- und Softwaresysteme korrekt funktionieren. Dazu wird einerseits beschrieben, was das System tun soll (die Spezifikation), und andererseits, wie das System funktioniert (das Modell). Beides wird in Formeln der mathematischen Logik übersetzt. Spezielle Software-Tools, sogenannte Reasoner oder Solver, prüfen dann, ob das Modell die Spezifikation erfüllt.

In der Praxis muss ein Kompromiss zwischen der Ausdrucksstärke dieser logischen Formeln und der Effizienz hergestellt werden, mit der Solver sie verarbeiten können. Für einfache Boolesche Logik gibt es heute sehr schnelle Solver. Für komplexere Probleme, insbesondere solche im Bereich der „Synthese“—also dem automatischen Erstellen eines Systems aufgrund einer Spezifikation—können die notwendigen logischen Formeln jedoch zu groß werden, um überhaupt in den Hauptspeicher eines Computers zu passen.

Dieses Projekt hat neue Methoden für ausdruckstärkere Logiken entwickelt, die sich für Syntheseaufgaben eignen. Diese Methoden betrachten Solver nicht nur als Algorithmen, die entscheiden, ob eine Lösung existiert, sondern als Algorithmen, die eine entsprechende Lösung auch konstruieren.

Eine wesentliche Errungenschaft unseres Projekts ist eine Technik, mit der Teile einer Spezifikation identifiziert werden können, deren Lösung eindeutig ist. Diese Methode ist ein zentraler Bestandteil eines neuen Reasoning-Tools für sogenannte Dependency Quantified Boolean Formulas (DQBF). Es versucht wiederholt, eine Lösung für die verbleibenden Teile der Spezifikation zu erraten, deren Lösung nicht eindeutig ist. Es prüft, ob diese Lösung korrekt ist, und modifziert sie, wenn das nicht der Fall ist. Dieses Tool kann beispielsweise dazu verwendet werden, um zu testen, ob zwei unvollständige Schaltkreise so vervollständigt werden können, dass sie dieselben Ausgangssignale haben.

Wir konnten außerdem zeigen, dass viele bekannte Entscheidungsalgorithmen für Quantified Boolean Formulas (QBF) von einem einzigen System subsumiert werden. Zudem haben wir bewiesen, wie ein besonders wichtiger von diesen Algorithmen so modifiziert werden kann, dass er Lösungen konstruiert.

Als wesentlichen Anwendungsbereich von QBFs haben wir die Minimierung von Schaltkreisen identifiziert. In unseren Experimenten konnten wir die Größe von für Anwendungen repräsentativen Schaltkreisen mitunter deutlich reduzieren, und dabei in einigen Fällen die ersten Verbesserungen seit Jahren erzielen.

Wir haben diese Methode vor kurzem in Software integriert, die in der akademischen Forschung und der elektronischen Designautomatisierungsbranche intensiv verwendet wird. Unsere Methode wird dadurch in Zukunft zur Produktion kleinerer und damit energieeffizienterer integrierter Schaltkreise beitragen.

Open Access Publikationen:

Slivovsky, F. (2020). Interpolation-Based Semantic Gate Extraction and Its Applications to QBF Preprocessing. In: Lahiri, S., Wang, C. (eds) Computer Aided Verification. CAV 2020. Lecture Notes in Computer Science(), vol 12224. Springer,

Cham. https://doi.org/10.1007/978-3-030-53288-8_24

Leroy Chew and Friedrich Slivovsky. Towards Uniform Certification in QBF. In 39th International Symposium on Theoretical Aspects of Computer Science (STACS 2022). Leibniz International Proceedings in Informatics (LIPIcs), Volume 219, pp. 22:1-22:23, Schloss Dagstuhl – Leibniz-Zentrum für Informatik (2022) https://doi.org/10.4230/LIPIcs.STACS.2022.22

Friedrich Slivovsky. Strategy Extraction by Interpolation. In 27th International Conference on Theory and Applications of Satisfiability Testing (SAT 2024). Leibniz International Proceedings in Informatics (LIPIcs), Volume 305, pp. 28:1-28:20, Schloss Dagstuhl – Leibniz-Zentrum für Informatik (2024) https://doi.org/10.4230/LIPIcs.SAT.2024.28

Franz-Xaver Reichl, Friedrich Slivovsky, and Stefan Szeider. eSLIM: Circuit Minimization with SAT Based Local Improvement. In 27th International Conference on Theory and Applications of Satisfiability Testing (SAT 2024). Leibniz International Proceedings in Informatics (LIPIcs), Volume 305, pp. 23:1-23:14, Schloss Dagstuhl – Leibniz-Zentrum für Informatik (2024) https://doi.org/10.4230/LIPIcs.SAT.2024.23

Wissenschaftliche Disziplinen:
Artificial intelligence (50%) | Theoretical computer science (50%)

Keywords:
Quantified Boolean Formulas, Artificial Intelligence, Machine Learning

---

Principal Investigator:	Friedrich Slivovsky
Institution:	TU Wien
Co-Principal Investigator(s):	Stefan Szeider (TU Wien)

Status: Abgeschlossen (01.05.2020 - 30.09.2024)
GrantID: 10.47379/ICT19060

Weiterführende Links zu den beteiligten Personen und zum Projekt finden Sie unter
https://wwtf.at/funding/programmes/ict/ICT19-060/