

ICT19-060 - Learning to Solve Quantified Boolean Formulas

Abstract

Mistakes in hardware and software can be expensive and cause major problems in the infrastructure we depend on every day. The area of formal methods focuses on proving that hardware and software systems work correctly. To do that, what the system should do (the specification) and a model of how the system operates are both written as formulas in mathematical logic. Special software tools, called automated reasoners or solvers, then check if the model meets the specification.

In practice, there is a balance between how expressive these logical formulas can be and how efficiently reasoners can process them. For simple Boolean logic, we now have very fast reasoners. However, for some problems—especially those involving “synthesis,” where we want to automatically create a system from its specification—the required logical formulas can become too large to fit into a computer’s memory.

This project developed new methods for more advanced kinds of logic that are suitable for synthesis tasks. These methods consider reasoners as tools that not only decide if a solution exists, but also help to construct that solution.

One of our key achievements was a technique for identifying parts of a system’s design for which the specification allows only a single solution. This method is an important component of a new reasoning tool for the logic of Dependency Quantified Boolean Formulas (DQBF). This tool repeatedly guesses a solution for the remaining parts of the specification, checks whether it is correct, and learns from its mistakes. For example, it can help determine whether two templates for integrated circuits can be completed so that they produce the same output.

We also showed that many existing algorithms for working with Quantified Boolean Formulas (QBF) can actually be combined into a single, unified system, and proved how solutions can be efficiently constructed for a well-known class of QBF reasoners.

Finally, as a practical application of these algorithms, we demonstrated that QBF can naturally represent the task of locally improving an integrated circuit by replacing certain parts of the circuit with smaller ones. In our experiments, we were able to shrink the sizes of circuits representative of industrial designs, in some instances finding the first improvement in years.

We have recently implemented it in a tool that is widely used in academia and the electronic design automation industry, where it will contribute to the production of smaller and thus more power efficient integrated circuits.

Open Access Publications:

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>

Scientific disciplines:

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: Completed (01.05.2020 - 30.09.2024)

GrantID: 10.47379/ICT19060

Further links to the persons involved and to the project can be found under

<https://www.wwf.at/funding/programmes/ict/ICT19-060/>