Short-Term Scientific Mission Grant
- APPLICATION FORM[1] -

Action number: CA20111

Applicant name: Martina SEIDL

Details of the STSM

Title: Checking proofs from QBF solvers in Dedukti and Lambdapi

Start and end date: 19/02/2024 to 23/02/2024

Goals of the STSM

To increase the trust in a result (SAT/UNSAT), SAT and quantified Boolean formulas (QBF) solvers produce certificates that can be independently checked [3]. The goal of this research visit is to determine whether Dedukti/Lambdapi could be used to check such proofs and what architecture could be used. We guess that the best solution would be to implement a tool that extracts subproblems from the certificate and reconstructs complete proofs in Dedukti as it is done by Ekstrakto for first order problems [1]. It has been shown that for main QBF proof systems it is possible to extract Skolem functions and Herbrand functions (which allow for the elimination of quantified variables) from proof; extractors have been implemented in CertCheck for example [2]. A complementary objective of the research visit would be to leverage Dedukti /LambdaPi to verify this extraction.

[1] Mohamed Yacine El Haddad, Guillaume Burel, Frédéric Blanqui. EKSTRAKTO A tool to reconstruct Dedukti proofs from TSTP files (extended abstract). PxTP 2019: 27-35

[2] Aina Niemetz, Mathias Preiner, Florian Lonsing, Martina Seidl, Armin Biere: Resolution-Based Certificate Extraction for QBF. SAT 2012: 430-435

[3] Martina Seidl: Never Trust Your Solver: Certification for SAT and QBF. CICM 2023: 16-33

Working Plan

his short-term mission is planned from Feb 19, 2024 to Feb 23, 2024 at University of Paris-Saclay. We want to realise the tasks described in the following.

1. Introduction to QBF proof systems

The first task consists of an in-depth introduction on the various QBF proof systems as produced by recent QBF solvers. The proof systems include Q-resolution [4], the QBF version of resolution for QBF, QRAT [2], the QBF version of the propositional RAT proof system, as well as FORALL-EXP-RES

[1] This form is part of the application for a grant to visit a host organisation located in a different country than the country of affiliation. It is submitted to the COST Action MC via e-COST. The Grant Awarding Coordinator coordinates the evaluation on behalf of the Action MC and informs the Grant Holder of the result of the evaluation for issuing the Grant Letter.

[3], a proof system for expansion-based QBF solvers. Further, all participants will be made familiar with tool chains as implemented in frameworks like QBFCert [5].

2. Architecture of the checking process with Dedukti/Lambdapi (DK/LP)

In this task, we evaluate the possibilities to use DK/LP to check QBF proofs. In particular, we will focus on the QBF proof system for which the available tool support fits best with the infrastructure provided by DK/LP. We will experiment with some formulas that are small enough to provide hand-crafted proofs. For example, we need to decide whether we start with true or with false formulas. While in theory, proofs for true and false formulas are dual for QBFs, in practical implementations there are some technical details that need to be taken into account. On this basis, we get a first impression of the feasibility of the approach. We will also take first steps towards the formalisation in lambdapi-calculus and Dedukti/Lambdapi.

3. Suitable benchmarks and first experiments

We will identify suitable benchmarks that allow us to evaluate our approach. These benchmarks should not be too easy and they should also not be too hard. For example, we could use application formulas from the QBFLib (www.qbflib.org), the community platform for QBFs, we could use crafted formulas [1], or we could randomly generate formulas. To choose a suitable benchmark set, we conduct first experiments.

4. Identification of next steps

This short-term mission is intended to employ Dedukti/Lambdapi for QBF proof checking. Important steps will be laid during the duration of this short-term mission. The ultimate goal is to provide a stable and competitive framework. It should be published at a suitable venue like IJCAR, CADE, SAT or a similar conference. We will identify the steps that need to be taken to achieve these objectives. Furthermore, we also will also identify further directions for collaboration like performance optimization or Skolem/Herbrand functions extraction.

[1] Olaf Beyersdorff, Luca Pulina, Martina Seidl, Ankit Shukla: QBFFam: A Tool for Generating QBF Families from Proof Complexity. SAT 2021: 21-29

[2] Marijn Heule, Martina Seidl, Armin Biere: A Unified Proof System for QBF Preprocessing. IJCAR 2014: 91-106

[3] Mikolás Janota, João Marques-Silva: On Propositional QBF Expansions and Q-Resolution. SAT 2013: 67-82

[4] Hans Kleine Büning, Marek Karpinski, Andreas Flögel: Resolution for Quantified Boolean Formulas. Inf. Comput. 117(1): 12-18 (1995)

[5] Aina Niemetz, Mathias Preiner, Florian Lonsing, Martina Seidl, Armin Biere: Resolution-Based Certificate Extraction for QBF. SAT 2012: 430-435

Expected outputs and contribution to the Action MoU objectives and deliverables.

This work contributes to the two following MoU objectives, " Express new systems into the Dedukti logical framework" and "Promote the output of detailed, checkable proofs from automated theorem provers". It is linked to WG1 and WG2 working groups.

The expected output is the design of an architecture to check proofs from QBF solvers by exploiting certificates emitted by QBF solvers and using Dedukti/LambdaPi and a prototype of a checker that would be continued in the future. In particular, we will provide the four deliverables related to the four work packages described above. The overall outcomes of this short-term mission will be documented in a detailed project report.

Deliverable 1: This deliverable will include all the resources used in the hands-on tutorial on QBF proof systems and certificates. This will involve slides as well as the artefacts (proofs, certificates) generated for training purposes.

Deliverable 2: Description of the envisioned architecture as well as first examples providing a proof of concept showing the feasibility of the proposed approach.

Deliverable 3: Formulas for which we aim to obtain a certified result as well as a description of outcomes of first experiments.

Deliverable 4: Description of the next steps. In particular, we will document how we plan to foster the started collaboration.