Report on the outcomes of a Short-Term Scientific Mission[1]

Action number: CA20111

Grantee name: Jesper Amilon

Details of the STSM

Title: Automatic verification of floating-point programs using Constrained Horn Solvers.

Start and end date: 11/09/2023 to 22/09/2023

Description of the work carried out during the STSM

Description of the activities carried out during the STSM. Any deviations from the initial working plan shall also be described in this section.

Overall, we worked on verification of floating point programs in the Eldarica Horn solver. The discussion mainly focused on how to verify programs by abstraction to rational numbers. From the verification, we then also discussed how to translate proof witnesses over the rationals back into the floating point domain. In this case, witnesses consists of solution to a set of constrained Horn clauses (CHCs). We also started implementing some of the discussions, as part of the theory for rational numbers in the Princess SMT solver (which is the back-end solver for Eldarica). Specifically, we realised how the current implementation of rational numbers should be refactored, in order to better allow back-translations of solutions.

During the visit, Philipp answered all and many of my questions regarding Horn solving, and SMT solving in general, as well as question regarding specific implementations in Eldarica/Princess.

Aside from the above mentioned, the visit also spurred some interesting discussions regarding probabilistic proofs of correctness for floating point programs. In particular, we discussed and experimented briefly with statistical methods for achieving probabilistic bounds for rounding errors in floating point arithmetics. The idea is that such probabilistic methods would complement the abstraction to rational numbers.

[1] This report is submitted by the grantee to the Action MC for approval and for claiming payment of the awarded grant. The Grant Awarding Coordinator coordinates the evaluation of this report on behalf of the Action MC and instructs the GH for payment of the Grant.

Description of the STSM main achievements and planned follow-up activities

Description and assessment of whether the STSM achieved its planned goals and expected outcomes, including specific contribution to Action objective and deliverables, or publications resulting from the STSM. Agreed plans for future follow-up collaborations shall also be described in this section.

(max. 500 words)

We fulfilled the overall goal, which was to discuss and plan the implementation of rational numbers, including backtranslation of proof witnesses, within the Eldarica/Princess tool-chain. The idea is to continue with finalising the implementation, and at the same time consider if any aspects of it can be published. In particular, we believe that the backtranslation of witnesses will lead to interesting results that may yield a publication. We also plan to continue working on the statistical/approximation approac for verifying round-off error that was mentioned in the previous section.

In the STSM proposal, we listed four specific outputs/contribution, and I will mention below how they were fulfilled.

1: RCO3: “Make techniques for program verification more effective and more accessible to all stakeholders.”
While no implementation is ready for use as a result of the visit, we now have a more clear picture of how to proceed in order to enhance the verification capabilities of Horn solvers.

2: “Bring together members of the different communities working on proofs in Europe.” During the visit, I could make use of Philipp’s knowledge within both SMT-solving and Horn-solving, and I have now a better picture as to how they can be utilized for example in a deductive verification context (which is my main research field).

3: “Act as a stakeholder platform in the field of formal proofs from its theoretical grounds to its industrial applications.
As mentioned in the proposal, the need for rational numbers comes from an industrial case study, and the visit certainly reaffirmed that utilising horn solvers can be useful in an industrial context for the purpose of verification floating point arithmetic.

4: “Create an excellent and inclusive network of researchers in Europe with lasting collaboration beyond the lifetime of the Action.”

The visit helped me connect with several new researchers, and it is likely that the visit can be one step towards future collaborations between research groups in Regensburg University and KTH..