Short-Term Scientific Mission Grant

- APPLICATION FORM[1] -

Action number: CA20111

Applicant name: Gergely Buday

Details of the STSM

Title: A bootstrapping verified compiler for a concurrent functional language: the design.

Start and end date: 11/04/2022 to 15/04/2022

Goals of the STSM

The goal of this STSM is to have an in-person meeting to develop and discuss the design of a verified compiler for a concurrent functional language. This work builds on top of Magnus Myreen's paper A Minimalistic Verified Bootstrapped Compiler, and we plan to add support for concurrency.

While we expect collaboration to happen remotely, we believe a few days of in-person interaction would be helpful to advance on such design. It would also be an opportunity for Buday to meet other researchers in our group and learn about other formalization alternatives.

The starting point of my research is. This describes a compiler written for a very simple untyped functional language. My plan is to extend this language with concurrency and bootstrap that compiler. The first step is to rewrite the language semantics from big-step to small-step semantics as concurrency needs that. Dr. Alcides Fonseca has expertise in concurrency so we can discuss the compiler design from that point of view.

Working Plan

During the 5-day visit we plan to:

- Discuss the structure of Myreen's compiler
- Define semantics of concurrency for the extended language, in particular the small-step semantics related to concurrency, channels, and events (all features of Concurrent ML)
- Identify the relevant theorems, related to desirable properties of concurrent programs (liveliness, deadlock-freedom)
- Discuss the theorem proving technologies that would be most useful for this task.

[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.

Funded by
the European Union

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

The main goal of the action is proof interoperability, and related technologies. Designing a certified compiler for concurrent programs is a very hot topic, in which proofs play a crucial role. Buday has experience in Isabelle and HOL4, while the host team has experience in Lean, Agda and SMT/Z3. By discussing designs and challenges, we hope to document the different advantages and disadvantages of each approach.

This work is particularly important for Buday, because of the lack of expertise in this area in his university. Collaborating with another group, with more expertise in theorem provers, would increase the productivity and quality of Buday's work.

The expected output is the detailed design of the proposed bootstrapping verified compiler for a concurrent functional language that can be implemented after the visit. This will be the focus of a joint publication, and an important chapter in Buday's PhD thesis.