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

Action number: CA20111

Grantee name: Emilio J. Gallego Arias

Details of the STSM

Title: **Sabanci** University Coq Workshop and Research Visit

Start and end date: 05/09/2022 to 18/09/2022

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.

The visit took place at the Sabanci Campus during two weeks, starting September 5th, 2022. We dedicated the **first week (5th--9th) to the planned Coq course**, increasing one day the planned schedule, and moved **the research part of the visit to the week after the course (12th-16th)**, due to availability of the host. Thus, the whole visit was shifted 5 days from its original schedule. The visitor was hosted in the Sabanci campus. We proceed to describe the activities in 2 separate sections:

Coq Course "Real World Coq":

The 5-day introductory Coq course proceeded as planned. The course had an attendance of **10 on-campus participants and 4 more persons by Zoom.**

Each day, we did a **3-hour lecture**, followed by a **2-hour exercise session** after lunch. The participants were an **even split of mathematicians and computer scientists**.

The focus of the class was on first having the participants understand **Coq's main ideas and become self-sufficient with the system**, then moving progressively towards an understanding of Coq's more advanced patterns and capabilities, including **software and mathematics verification**.

We think that the course was successful, and achieved its main goal to **introduce to the audience the theory and applications of interactive proof assistants**. Teaching was done on a **shared, interactive document for each session**, and we did spend considerable time doing proofs together, thanks to the small class size.

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.

The material and meta-data for the course **is available** at https://ejgallego.github.io/real-world-coq/ ; the classes were also recorded, and we may make them available soon, tho we think the format we used may not be the most attractive to self-learners due to the lengthy in-class discussions and joint proof development.

We didn't cover all the material we had planned, as some of the topics required more time than planned. The course was also very fruitful in terms of interactions with the attendees.

Research discussion:

For the second week of the STSM, host and visitor **meet every day**. After our interactions at the course, we chose to explore the **development of a joint Coq library prototype to model state-of-the-art automatic verification techniques familiar to the host to establish properties of distributed systems**. This line of work was motivated by the complexity of some of these proofs, in particular by the observation of some recent papers where t**he review process had struggled** in this sense; and also motivated because the foundational verification of such systems by ITPs such as Coq, Lean, or Isabelle with reasonable effort is still **an open problem.**

As the core reference, we took Suha's PLDI 2020 paper ``**Inductive Sequentialization of Asynchronous Programs**'' (https://hal.archives-ouvertes.fr/hal-03597589/document), implementing two simpler protocols in Coq (**ping-pong** and **leader election**), and their corresponding ``moves'' in terms of the network model.

I also gave a **department-wide seminar on Sep. 12th**, presenting recent work on the v**erification of Economic Mechanisms in Coq,** using a foundational relational logic, and discussed further with several students and faculty.

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.

We think the STSM achieved our original goals and expectations, and we had a fruitful and fun visit both as a host and visitor.

On the course side, we achieved two core goals:

- to introduce **state-of-the-art interactive theorem proving** to an unfamiliar audience
- to gather **important feedback about the course and the teaching material we produced**, with the aim of maturing this new Coq course.

The first point directly contributed to Capacity Building Objectives **"4. Ease access to formal verification techniques in education and other areas of science."** and "**5. Actively support young researchers, the under-represented gender, and teams from regions with less capacity."**

In particular, ITP tools have not yet seen widespread adoption in Turkey, and this intensive course was given to *both young faculty* and *master and PhD students*, with very positive feedback in terms of whether they will remain interested in interactive formal proofs in the future.

The opportunity to teach this class in such intensive format was of great help to identify particular problematics on the teaching methods and tools for Coq and for other similar interactive proof assistants. Thus, we can say that the class was of mutual benefit, as it is expected.

For instance, and in accordance with *our own expertise on user interface design for ITPs*, we used our

own jsCoq system for live teaching, and we identified many problems and missing features in that setting. Problems particularly relate to the **exploration and understanding** of coercions, structures, theories, and notations; we have designed remediations accordingly, and incorporated them to the roadmap of our tool. We think both **the tool and lessons learned** here are of **general interest for the participants of the Cost action.**

Regarding the course contents and material, the scope of the syllabus was **quite ambitious** for the amount of time available, but again the feedback was very valuable. We plan to refine the current material, hoping to do a second iteration of the course in **Spring 2023**. All the materials will remain publicly available.

We are also satisfied with the second week, pertaining the formalization of automated verification techniques for distributed systems in Coq.

We believe our work directly targets point **"6. Transfer knowledge in terms of expertise, scientific tools and human resources across the different disciplines and between academia and industry.**", with a potential impact also on **"3. Make techniques for program verification more effective and more accessible to all stakeholders."**

We plan to **continue the collaboration with weekly online meetings**, and we have been exploring some options to further strengthen the collaboration such as the "Tubitak-France Bosforo Program".

We also meet Aysegul Rana Erdemli, about a potential joint supervision of her master internship (at Sabanci)

We have thus agreed to continue the development of the Coq formalization of the PLDI 2020 paper, using the techniques outlined in the course, (in particular the methodology developed by the Mathematical Components Team at Inria), hoping to **jointly supervise a student** so we complete the required manpower for a paper on this topic.