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

Action number: CA20111

Applicant name: Paola Giannini

Details of the STSM

Title: **Using *behavioural types* for automatic validation of distributed systems**

Start and end date: 19/09/2022 to 30/09/2022

Travel cost: 350 € + 50 € for internal travel (to/from airport etc.)

Accommodation cost: 988 €

Living cost: 30 € x14=420 €

Requested grant: 1800 €

Goals of the STSM

The purpose of the visit is to start a collaboration between the applicant and its research group on “Formal Methods for Software Development” and the research group “Models and Applications of Distributed Systems” (of which Laura M. Castro is a member). In particular, we intend to apply some of the type-theoretic techniques developed in the area of "multiparty-session-types" based coordination for distributed actor systems, the area of expertise of the applicant, to the verification and validation of distributed systems, the area of expertise of the host. In the visit we will try to identify case studies to support the use of hybrid techniques of verification type-theoretic and verification. The long term goal would be to mechanize type checking support to property testing and model checking for languages such as Erlang/Elixir.

Working Plan

A *multiparty session* forms a unit of structured communication among many participants which follow communication sequences specified as a *global type*, see [6]. The behaviour expected by the participants is expressed by *session types* which are obtained as projection from global type. If the processes associated to the participants behave as the session type obtained by projection the multiparty session has the properties of deadlock freedom and progress (lack of starvation and unread messages). The research group of the applicant proposed some enhancements of global types to adapt them to the description of more complex systems including the possibility of rolling back to named checkpoints, see [4], without losing the good properties of the multiparty session. Moreover in [5] the global types are extended to describe asynchronous sessions where participants interact by message passing. This is the computation model of *actor systems* and shared by the languages Erlang and Elixir.

Distributed concurrent systems in addition to properties of the interaction between their participants, expressible by global types, have other emerging properties which require hybrid approaches to their

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.

verification, from property testing to model checking, see [1]. In [2] and [3] it is proposed a formalisation that combines both model checking and property-based testing techniques using rewriting logic.

The aim of the collaboration between the applicant and the host would be to use the type-theoretic specification given by global types to provide guidance in the identification of the parts of the process codes which are related to some specific properties, in order to improve property testing and runtime verification for projects implemented as actor systems written in Erlang/Elixir.

In this first visit, the applicant and the host will give some seminars to familiarise each other and their collaborators with their respective areas of expertise and the tools used in such areas. Then,

- on one side we would try to identify the requirements that a system would have to meet in order to be of interest and select some project to be used as case studies, and

- on the other analyse the tools to support the formalisation/mechanisation used by the applicant and the host group.

A report on these activities will be produced.

References:

[1] Ammar Boucherit, Laura M. Castro, Abdallah Khababa, Osman Hasan: Towards the Formal Development of Software Based Systems: Access Control System as a Case Study. Inf. Technol. Control. 47(3): 393-405 (2018)

[2] Ammar Boucherit, Abdallah Khababa, Laura M Castro: Automatic generating algorithm of rewriting logic specification for multi-agent system models based on Petri nets. Multiagent and Grid Systems 14(4): 403-418 (2018)

[3] Ammar Boucherit, Laura M. Castro, Osman Hasan, Abdallah Khababa: Towards a hybrid formal analysis technique for safety-critical software architectures. Int. J. Crit. Comput. Based Syst. 10(2): 95-119 (2021)

[4] Ilaria Castellani, Mariangiola Dezani-Ciancaglini, Paola Giannini: Reversible sessions with flexible choices. Acta Informatica 56(7-8): 553-583 (2019)

[5] Francesco Dagnino, Paola Giannini, Mariangiola Dezani-Ciancaglini: Deconfined Global Types for Asynchronous Sessions. COORDINATION 2021: 41-60

[6] Kohei Honda, Nobuko Yoshida, Marco Carbone: Multiparty asynchronous session types. POPL 2008: 273-284

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

The proposed STSM is relevant to Working Group 3 on Program Verification.

In the long term, the contribution goes towards the objective of making techniques for program verification more effective and more accessible to all stakeholders.

In the short term, as mentioned in the Working Plan, we would like to identify
- system properties that could take advantage by the use of types in conjunction with property testing and model checking
- some case studies from the industrial world to apply the hybrid techniques
- tools which better support the previous points.

Moreover, the type-theoretic techniques, could be of interest, as case study, for the Working Group 6 on Type Theories