EUROPEAN COOPERATION
IN SCIENCE & TECHNOLOGY

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

Action number: CA20111

Applicant name: Daniele Nantes Sobrinho

Details of the STSM

Title: Higher-Order Equational Unification and Anti-Unification for Program Verification

Start and end date: 17/March/2025 – 27/March/2025

Detail of the cost in EUROS:

- Transport (upload screen capture): 155 euros (£129)

- Hotel/day (upload screen capture): 15 euros (150 euros total – accommodation at the university)

- Food/day: 40 euros (400 euros total)

TOTAL: 705 euros

Goals of the STSM

Purpose and summary of the STSM.

*This STSM aims to foster research collaboration between Daniele and David Cerna. The primary focus is on advancing nominal equational anti-unification methods. The proposal builds on David's prior research on anti-unification for higher-order patterns, as presented in [*Cerna and Kutsia, 2020*]. Specifically, the objective is to extend the nominal framework introduced in [Schauß and Nantes, 2022] by integrating support for equational theories, further developing the work started in [Schauß and Nantes, 2023], leveraging David's proposed approach. Additionally, this work seeks to explore the relationship between anti-unification in higher-order patterns and nominal anti-unification, as suggested by existing connections in the context of unification [*Levy and Villaret, 2012*].*

A secondary goal of the visit is to collaborate on schematic unification, which has practical applications in program verification, and it is part of Daniele's ongoing research [Lööw and Nantes et. al.,2024a]. This includes designing a matching algorithm for static analysis for software verification based on separation logic, with particular emphasis on languages that include recursive predicates [Lööw and Nantes et al., 2024b].

Working Plan

Description of the work to be carried out by the applicant.

The plan is to hold regular meetings over the 10-day visit with David Cerna. The topics of these meetings will be those mentioned in the previous section. Also, Daniele plans to dedicate part of her time investigating how the current Coq formalisation of the matching algorithm for separation logic can be adapted to include recursive predicates following David's approach to schematic unification. The point of

[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.

this visit is to hold several focused discussions on the topics mentioned above and to work towards writing up ideas and solutions discussed over the past several months.

References:

[Cerna and Kutsia, 2020] David M. Cerna, Temur Kutsia, Higher-order pattern generalization modulo equational theories. Math. Struct. Comput. Sci. 2024

[*Schauß and Nantes, 2022*] Nominal Anti-unification with Atom-Variables. FSCD 2022.

[*Schauß and Nantes, 2023*] Towards Fast Nominal Anti-unification of Letrec-Expressions. CADE 2023.

[Levy and Villaret, 2012] Nominal Unification from a Higher-Order Perspective. ACM Transactions on Computional Logic, 13(2), 2012.

[Lööw and Nantes et. al., 2024a] Compositional Symbolic Execution for Correctness and Incorrectness Reasoning. ECOOP 2024.

[Lööw and Nantes et. al., 2024b] Matching Plans for Frame Inference in Compositional Reasoning. ECOOP 2024.

[Cerna and Kutsia, 2023] David M. Cerna, Temur Kutsia: Anti-unification and Generalization: A Survey. IJCAI 2023

[Pientka, 2009] Brigitte Pientka. Higher-order term indexing using substitution trees. ACM Trans. Comput. Log., 2009.

[Parsert and Polgreen, 2024] Reinforcement Learning and Data-Generation for Syntax-Guided Synthesis. AAAI 2024

[Winter et al., 2022] Emily Rowan Winter, et. al. Towards developer-centered automatic program repair: fndings from Bloomberg. ESEC/FSE. ACM 2022.

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

Main expected results and their contribution to the progress towards the Action objectives (https://europroofnet.github.io/objectives/) and deliverables (https://europroofnet.github.io/deliverables/).

Working groups to which this mission contributes:

Daniele anticipates that at least one of the aforementioned topics will be partially addressed during the 10-day period, with measurable progress toward a technical report. The work completed during this time is expected to form the basis of a submission to one of the major reasoning conferences with a submission deadline in July 2025. Regarding contribution to the action's objectives, anti-unification is an important operation (as outlined in [Cerna and Kutsia, 2023]) with applications within many of the tools addressed in the MoU objectives list and deliverables. For example, it is used for the extraction of substitutions from substitution trees [Pientka, 2009], for applications of machine learning to synthesis problems [Parsert and Polgreen, 2024], and program repair [Winter et al., 2022].

Unification, a cornerstone of automated reasoning, has broad applications in automated theorem proving and program verification. For example, the research described in [Lööw and Nantes et al., 2024a] is implemented in the Gillian tool, which is used for static analysis and has been applied to verify AWS code. This work is currently undergoing formalization in Coq.

Working Groups: WG2, WG3 & WG5.