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

Action number: CA20111

Applicant name: Roland Herrmann

Details of the STSM

Title: Array logics and aggregation functions for program verification

Start and end date: 09.03.2025 - 16.03.2025

Detail of the cost in EUROS:

- Transport: 472 euro

- Hotel/day: 134 euro

- Food/day: 30 euro

TOTAL: 1784 euro

Goals of the STSM

Purpose and summary of the STSM.

Our current work focuses on the satisfiability problem of array logics, with particular attention to aggregation functions like min/max or summation over all array elements—an area that has received little attention so far. Recently, we developed a decision procedure for the quantifier-free fragment of formulas involving the standard signature of McCarthy-style arrays, constant array operators and constraints on the sum of array elements. While its implementation into an SMT solver is still ongoing, we are exploring potential applications for this procedure.

One promising direction stems from a 2023 CAV paper by the theoretical computer science group at KTM in Stockholm [1], which discusses automatic verification through instrumentation. Their approach involves rewriting program specifications, but for array formulas, they currently lack a decision procedure for handling aggregation functions in the resulting program specifications. Our main goal is to investigate how our decision procedure could be integrated into their framework to support reasoning about rewritten specifications, possibly integrating also other aggregation functions needed.

[1] Amilon, J., Esen, Z., Gurov, D., Lidström, C., Rümmer, P. (2023). Automatic Program Instrumentation for Automatic Verification. In: Enea, C., Lal, A. (eds) Computer Aided Verification. CAV 2023. Lecture Notes in Computer Science, vol 13966. Springer, Cham. https://doi.org/10.1007/978-3-031-37709-9_14

(max.200 word)

Working Plan

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

At first we present our current research on our respective topic, either on further research beyond the

[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.

published paper [1] or the developed decision procedure and decidability results on array logics. Taking those discussions into account there are three directions to work on.

1. We will integrate the already developed decision procedure on arrays with sum constraints into the problem of reasoning about program specifications mentioned in the CAV paper.
2. We investigate if and how the decision procedure on arrays with sum constraints can be extended to other aggregation functions. We try to recognize an as big as possible class of functions for which this is possible. Eventually this may result in adapted decision procedures for different classes of aggregation functions.
3. We will evaluate the performance of our decision procedure using benchmarks taken from the CAV 2023 paper, and refine our approach to address potential performance issues.

We will evaluate which directions are the most promising for further research. This includes identifying cases where certain approaches may not be feasible or developing initial strategies for those that show potential.

(max.500 word)

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

Main expected results and their contribution to the progress towards the Action objectives (either research coordination and/or capacity building objectives) and deliverables.

Working groups to which this mission contributes: WG3 Program verification

We anticipate mutual benefits from combining our two perspectives on aggregation functions: one focused on the theoretical development of decision procedures for satisfiability problems, and the other driven by practical needs in program verification use cases. Our goal is for this initial visit to lay the foundation for a long-term collaboration on this topic, fostering a strong connection between the two departments.

The outlined directions for our work are concrete and diverse, increasing the chances of making meaningful progress across multiple aspects. While each direction involves its own challenges, they provide clear paths to explore promising ideas, with potential to advance both theoretical understanding and practical applications.

By pursuing these efforts, we contribute to the following objectives of the Action:

- *Create an excellent and inclusive network of researchers in Europe with lasting collaboration beyond the lifetime of the Action*
- *Bring together members of the different communities working on proofs in Europe*

(max.500 words)