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

Action number: CA20111

Applicant name: Sibylle Möhle-Rotondi

Details of the STSM

Title: Model Representation Formalisms for Constrained Horn Clauses over Algebraic Data Types

Start and end date: June 16, 2025 – June 27, 2025

Detail of the cost in EUROS:

- Transport (upload screen capture): 188.12 (refundable)

- Hotel/day (upload screen capture): 108.50 (refundable until June 7, 2025)

- Food/day: 64

TOTAL: 2'539.12

The applicant will visit the Laboratory for Automated Reasoning and Analysis (LARA) led by Viktor Kunčak at EPFL, where she will collaborate with Viktor Kunčak and Sankalp Gambhir, who is submitting a complementary STMS proposal for visiting University of Regensburg.

Goals of the STSM

In formal verification, a program and the required correctness properties may be translated into verification conditions expressed as sets of constrained Horn clauses (CHCs) over the background theory of algebraic data types (ADTs) which are analysed for checking the correctness of the program. The solutions of sets of CHCs represent loop invariants or pre-/post-condition of functions and can be computed by standardised CHC solvers. However, existing CHC solvers often are unable to represent solutions of examples of CHCs involving inductively defined data structures, whereas in the area of automated model building representation formalisms exist which can represent recurrent structures like those occurring in solutions of CHCs with ADTs. Therefore, the applicant is working on developing new techniques for the representation and computation of solutions of CHCs over ADTs by combining algorithms and tools from the field of CHC solving with techniques from the area of automated model building.

The purpose of the STSM is to develop new model representation formalisms for solutions of CHCs over ADTs suited for improving the expressiveness of invariants and constraints.

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.

Working Plan

We develop new techniques for the representation and computation of *non-elementary* solutions of CHCs over ADTs, i.e., solutions which can not be expressed by quantifier-free formulae in the background theory of ADTs. For developing model representation formalisms for ADTs, we build on existing work in automated model building and in the broader context of automated reasoning where the focus is on a finite representation of infinite models. The new formalisms shall meet the model building postulates by Carerra et al. [1]. These postulates describe general conditions on the output of model building procedures and also provide a measure for the computational processability of a representation. We investigate further properties, such as closedness under intersection (which is met by elementary representations).

One goal is to represent models over recursively defined data types, such as lists. One possibility is to enrich elementary representations by functions which can be refined through (primitive) recursion on ADTs. From a model, recursive functions describing the computation and inductive invariants can be extracted [2]. We will also consider ADTs extended with a wider range of recursive functions, including functions to count individual constructors or the occurrences of specific sub-terms, each of which gives rise to a new class of models. A general framework in which decidability is preserved for such extensions are the *sufficiently surjective functions* developed by Suter et al. [3], which will be one of our starting points.

A further promising candidate is the language clausal monadic shallow linear Horn (MSLH) [4], a decidable fragment of first-order logic which has not yet been considered as a formalism for representing models of sets of CHCs. MSLH is a promising language due to its decidability and since its clauses are already Horn and thus close to CHCs. The task will be to enrich MSLH clauses by appropriate constraints.

These ideas target solving problems which occur in practice. However, we also aim at obtaining a theoretical understanding of CHC solving over (recursive) ADTs. To achieve this goal, we plan to also investigate solvability rather than providing concrete models, according to *proof-theoretic semantics.* This view is more general than the one of *model-theoretic semantics,* in which evidence is given by a concrete model, and which is commonly used.

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

Our results will be of theoretical nature and of interest for research groups working in topics in which the representation of models in first-order logic is essential. For instance, automated theorem provers are often restricted to find and represent finite models. We expect that our results can contribute to detecting infinite models in automated theorem proving (ATP). The new model representation formalisms will further allow to find more expressive invariants and thus provide directions for extending the theory of ADTs supported by the Eldarica Horn solver [5]. We expect that the theoretical understanding of CHC solving will support the search for more expressive invariants further. Due to the use of automated theorem provers and CHC solvers in academic and industrial applications, our results are also of practical relevance.

Our deliverables consist of model representation formalisms for ADTs and a detailed investigation of their properties as well as the relation between them. With this work, we directly contribute to the Action objective “Make techniques for program verification more effective and more accessible to all stakeholders” and on a longer-term basis to “Promote the output of detailed, checkable proofs from automated theorem provers”.

With this STSM, we expect to develop the applicant’s and host’s network and to initiate long-term fruitful collaborations by combining and learning from the applicant’s and coworker’s expertise. As mentioned above, we expect that different communities will benefit from our work on model representation formalisms. We therefore contribute to the capacity building objectives “Bring together members of the different communities working on proofs in Europe” and “Create an excellent and inclusive network of researchers in Europe with lasting collaboration beyond the lifetime of the Action”.

Working groups to which this mission contributes: WG3 Program Verification

References

[1] Ricardo Caferra, Alexander Leitsch, and Nicolas Peltier. Automated Model Building. Kluwer, 2004.

[2] Lucas Zavalía, Lidiia Chernigovskaia, and Grigory Fedyukovich. Solving constrained Horn clauses over algebraic data types. In VMCAI, vol. 13881, LNCS, pp. 341–365. Springer, 2023.

[3] Philippe Suter, Mirco Dotta, and Viktor Kunčak. Decision procedures for algebraic data types with abstractions. In POPL, pp. 199–210. ACM, 2010.

[4] Christoph Weidenbach. Towards an automatic analysis of security protocols in first-order logic. In CADE, vol. 1632, LNCS, pp. 314–328. Springer, 1999.

[5] Hossein Hojjat and Philipp Rümmer. The ELDARICA Horn solver. In FMCAD, pp. 1–7. IEEE, 2018.