cost
EUROPEAN COOPERATION
IN SCIENCE & TECHNOLOGY

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

Action number: CA20111

Applicant name: Jasper Nalbach

Details of the STSM

Title: SMT solving and proofs for non-linear arithmetic

Start and end date: 28/08/2023 to 08/09/2023

- 28th August 2023-1st September 2023 Bath
- 4th September 2023-8th September 2023 Coventry

We are aware that the requested funding is high compared to the average STSMs funding. Since our funding is currently scarce, we will appreciate from COST any reasonable help, and we will cover the remaining from other sources. We will be able to stick to our proposal with 2k€ of COST funding.

Goals of the STSM

Purpose and summary of the STSM.

Satisfiability-modulo-theories (SMT) solving is a technique for checking the satisfiability of (quantifier-free) first-order formulas over various theories. Witnessing satisfiability of a formula is as simple as returning an assignment; witnessing unsatisfiability requires a proof. Recently, the SMT solver cvc5 has been extended for producing proofs for many theories [1], but not yet for non-linear real arithmetic (NRA), the theory where the atoms consist of polynomial constraints.

The NLSAT algorithm introduced a conflict-driven search for NRA formulas, turning out to be highly efficient. Shortly after, a flourishing cooperation emerged between Aachen (Erika Ábrahám), Bath (James Davenport), Coventry (Matthew England) and others in the context of the SC^2 project, transferring ideas from computer algebra to SMT solving and vice versa. This cooperation led to the state-of-the-art CAIC [2] method (implemented in cvc5 [4]). Recent cooperation led to a (high-level) proof system for single cell construction [3] (a central building block of conflict-driven NRA algorithms) by Jasper Nalbach (PhD student at Aachen).

James Davenport is currently investigating how best to fill the gap between the proof system and computer-verifiable proofs. To support this, the goal is to extend the proof system for the CAIC method, increase its efficiency and applicability by incorporating new results from CAD theory.

[1] Barbosa, H. et al., “Flexible Proof Production in an Industrial-Strength SMT Solver”, IJCAR 2022,

[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.

https://doi.org/10.1007/978-3-031-10769-6_3

[2] Erika Ábrahám, James H. Davenport, Matthew England, Gereon Kremer, “Deciding the consistency of non-linear real arithmetic constraints with a conflict driven search using cylindrical algebraic coverings”, JSC, 2021, https://doi.org/10.1016/j.jlamp.2020.100633

[3] Jasper Nalbach, Erika Ábrahám, Philippe Specht, Christopher W. Brown, James H. Davenport, Matthew England, “Levelwise construction of a single cylindrical algebraic cell”, preprint on arXiv, 2022, https://doi.org/10.48550/arXiv.2212.09309

[4] G. Kremer, E. Ábrahám, M. England, J. H. Davenport, "On the Implementation of Cylindrical Algebraic Coverings for Satisfiability Modulo Theories Solving", SYNASC 2021, https://doi.org/10.1109/SYNASC54541.2021.00018

Working Plan

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

During our discussions, we will focus on the following topics:

- Extension of the proof system: We plan to exchange ideas on extending the proof system to include the CAlC method, and possibly CAD, to generate high-level proof graphs for NRA formulas.
- Current state of the proof system: We will discuss the current state of the proof system and the gap that exists for formal proofs in NRA. Our aim is to optimize the proof system to support filling that gap.
- Recent results from CAD theory: We will also discuss recent findings in CAD theory, specifically the Lazard projection operator, and explore how these results can be integrated into the proof system. By doing so, we hope to increase the applicability of the proof system to more formulas and potentially improve its efficiency, making it more likely to find formal proofs.

A further purpose of this stay is to collaborate with Lucas Michel (who applies separately), and the discussions we have will be shared between us. We have planned to spend one week at Bath with James Davenport (28th August 2023-1st September 2023) and extend our stay by joining Matthew England in Coventry (4th September 2023-8th September 2023 Coventry) to continue our discussions.

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.

Our team aims to leverage the strengths of Jasper Nalbach's high-level proof system and James Davenport's work on formal proofs by identifying synergies between the two. To achieve this, we will closely coordinate and synchronize our future work.

Lucas Michel, who recently began his PhD at Liège, will be introduced to the CAD theory and proof system. We plan to collaborate further, particularly in the scope of a DFG-FNRS project, to accelerate the development in this area. With the close proximity of Liège, Aachen, and the UK, we anticipate a tight collaboration in the future.

The ultimate outcome will be a set of theories, techniques and tools for production of proofs from SMT solvers (and automated reasoners in general) also when non-linear arithmetic reasoning is involved. These general goals contribute in particular to the EPN Objective 2 (Promote the output of detailed, checkable proofs from automated theorem provers), and D4 (Software for translating proof formats used by automated theorem provers to Dedukti).