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

Action number: CA20111

Applicant name: Lucas MICHEL

Details of the STSM

Title: Proof calculus for Real Algebraic Geometry

Start and end date: 28/08/2023 to 08/09/2023 (We are aware that the requested funding is high compared to the average STSMs funding. 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 for the variables; witnessing unsatisfiability requires the computation of 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. Producing replayable proofs for polynomial constraints is still an open and hard problem. There is nothing as universally usable as Farkas' lemma for proofs in linear arithmetic, when considering non-linear constraints.

The Aachen team, together with James Davenport and Matthew England have been recently working actively towards this goal, particularly to output some kind of proof trace detailing the reasoning within the CAIC method [2]. In parallel, and complementary to this approach the applicant (who has a mathematical background) will study proofs for non-linear decision procedures in a more global way, using relevant mathematical tools from Computational Real Algebraic Geometry. A first goal is to understand the details of the proof system from Nalbach's proof system [3]. Second, we aim to study how this system can be extended to accommodate other reasoning techniques for non-linear arithmetic (e.g., Gröbner basis, virtual substitution). Third, we would like to understand if there are ways to simplify proof output in the context of non-linear arithmetic reasoning. The grail would be to uncover some equivalent concept to Farkas' lemma, for non-linear arithmetic.

[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.

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

Working Plan

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

The working plan is as follow:

- Understand Nalbach's proof system (discussion with Nalbach and Davenport);
- Get up-to-date to the current status of Davenport's research on filling the gap between the proof system and computer-verifiable proofs;
- Discuss with Davenport and England on other aspects of non-linear reasoning;
- Plan the work on integrating other aspects of non-linear reasoning with Nalbach's proof system.

Additionally, Lucas Michel will discuss (with Davenport, England, and Nalbach) theoretical decision procedures (for instance, the critical point methods) that do not yet have any implementation, and the opportunity to implement them.

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.

Lucas Michel, obtained in September 2022 his Master in Mathematics, and started his PhD at Liège. He has learned the major techniques for non-linear reasoning and has already met shortly the Aachen team and James Davenport. We expect from this longer visit that he will get a better grasp at the challenges, the techniques, and the unexplored areas for non-linear reasoning and production of proofs for non-linear arithmetics. We believe having a mathematician PhD student focusing on these aspects will be a crucial help to the group of people studying non-linear arithmetic decision procedures for automated reasoning. There is a plan to collaborate further (UK, Aachen, and Liège teams), 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).