D. Gurov

/ DILIAN GUROV /

Report on the outcomes of a Short-Term Scientific Mission[1]

Action number: CA20111

Grantee name: Roland Herrmann

Details of the STSM

Title: Array logic and aggregation functions for program verification

Start and end date: 02/03/2025 to 09/03/2025

Description of the work carried out during the STSM

Description of the activities carried out during the STSM. Any deviations from the initial working plan shall also be described in this section.

We began with a mutual presentation of our current research to ensure a clear understanding of the different perspectives involved. On one hand, we work with C programs, where variables evolve over time due to sequential execution. On the other hand, the formulas used in our decision procedure lack explicit temporal dependencies in general. Additionally, MonoCera operates on partial sums with well-defined lower and upper bounds on the summation indices, whereas our decision procedure only supports sums over entire arrays. To bridge this conceptual gap, we studied the translation between these two perspectives in depth.

As a starting point, we restricted our focus to C programs that use for-loops as their primary control structures. Our initial approach aimed to leverage the decision procedure to verify whether the backtranslation of invariants generated by MonoCera for a given C program were indeed sufficient to imply the program's original specifications. However, we encountered a significant challenge: when the number of iterations in a for-loop is variable, this can lead to partial sums with an unknown number of summands, which is undecidable in general and falls outside the capabilities of our decision procedure. Addressing this limitation would require major modifications to our existing decision procedures.

Given these challenges, we shifted our focus to the opposite direction—rather than using our decision procedure to verify MonoCera's results, we explored how MonoCera could be utilized to enhance the efficiency of our decision procedure. We observed that our current decision

[1] This report is submitted by the grantee to the Action MC for approval and for claiming payment of the awarded grant. The Grant Awarding Coordinator coordinates the evaluation of this report on behalf of the Action MC and instructs the GH for payment of the Grant.

procedure struggles with handling logical formulas that arise from for-loops, as it essentially unfolds the loop step by step, leading to inefficient computations.

To overcome this, we developed the idea of using MonoCera to compress a for-loop into a single loop invariant before applying our decision procedure. Initial experiments demonstrated that MonoCera is particularly effective at identifying loop invariants, even when the number of iterations is variable. By replacing for-loops with the corresponding loop invariants and their associated partial sums, the translation of C programs into logical formulas becomes significantly more manageable. While our decision procedure does not yet fully support this approach, we are optimistic that only minor adjustments will be necessary to ensure soundness and correctness.

This approach not only integrates the strengths of both tools—MonoCera for finding loop invariants and our decision procedure for reasoning about array-based properties—but also holds promise for accelerating program verification through a more efficient handling of iterative constructs.

Apart from the specific research project, Dilian Gurov and Jesper Amilon provided insights into other projects within the theoretical computer science group at KTH and their respective research interests, which is always valuable for broadening one's horizons.

(max. 500 words)

Grantee enters max 500 word summary here.

Description of the STSM main achievements and planned follow-up activities

Description and assessment of whether the STSM achieved its planned goals and expected outcomes, including specific contribution to Action objective and deliverables, or publications resulting from the STSM. Agreed plans for future follow-up collaborations shall also be described in this section.

The STSM provided valuable insights into each other's perspectives on sums, fostering a deeper mutual understanding. Our discussions were particularly effective in clarifying misconceptions and efficiently establishing common ground. While our initial approach—verifying the validity of MonoCera's invariants through our decision procedure—proved somewhat feasible, our intensive collaboration throughout the week led to an even more promising alternative that had not been previously considered.

The key outcome of the STSM was the idea of leveraging MonoCera's efficiency in identifying loop invariants to accelerate verifying C-programs by our decision procedure. Instead of directly verifying invariants, we propose compressing only the for-loops into a single loop invariants, significantly simplifying the number of explicit indices occurring in the translated formula. Initial examples have been formulated on paper.

The next phase involves evaluating the loop invariants generated by MonoCera to determine whether they are sufficient to fully replace the original for-loops. If so, modifications to the decision procedure will be necessary, particularly in tracking which array segments are represented by the invariant—especially when they interact with other formula components. If the invariants are too weak we need to call MonoCera again with stronger assumptions to obtain

better invariants.

While soundness of the verification process is not expected to become a problem, we anticipate a potential loss of completeness, as summations with variable bounds is undecidable in general. To address this, further constraints on for-loop ranges must be considered to ensure the verification process remains complete.

A follow-up meeting is already planned, and we are optimistic that our approach will prove effective.

Furthermore, the insights into the other areas in which the theoretical computer science group at KTH is working stimulates possibilities for further research projects and new perspectives.

(max. 500 words)

Grantee enters max 500 word summary here.