Second WG3 Meeting

Report

WG leaders: Mădălina Erașcu and Alicia Villanueva

Context

The second WG3 meeting was planned as a two-day meeting to bring together members of the different communities working on proofs and verification in Europe. It was held at the West University of Timisoara, Romania. We thank the local organisers for their work and effort that contributed to having a successful event. The goals of the meeting were to:

- bring together members of the different communities working on proofs and verification,
- foster collaborations and build synergies among participants to ease the path to more fruitful results for the Action,
- work towards the deliverables which are due in 2023:
  - D5 (month 18): Comparison of the approaches used in the Software Verification competition SV-COMP.
  - D6 (month 24): Software prototype for the inference of program specifications as logical axioms.

Participation and Program

The meeting was announced through the official mailing lists epn-all@inria.fr, epn-wg3-verif@inria.fr, the Zulip channel (https://epn.zulipchat.com) and on the Action webpage (https://europroofnet.github.io/). The call was launched at the beginning of December with a deadline in the beginning of January. Since the winter holidays were not a beneficial time for applications, we extended the deadline after mid January. We had 21 on site participants and 4 online (https://europroofnet.github.io/_pages/WG3/Feb2023/ParticipantsWG3Timisoara.pdf). 20 participants were funded by the action and all of them were or became members of the action. The affiliation of the attendees were European universities, but some were affiliated with companies also, e.g. runtimeverification (https://www.runtimeverification.com/)

The program of this event (available at https://europroofnet.github.io/wg3-meeting-timisoara-program/) started with the presentation of the COST Action in general and the presentation of the WG3 goals and deliverables. Since there are two deliverables which are due in 2023, the program was structured around the topics of the 2 deliverables: the first day was dedicated to talks and discussions related to tools for software verification, the second on program specifications as logical axioms.

Output

One of the outputs of this event was the dissemination of the research results of the speakers with the aim of:

- building collaborative synergies.
- finding out how they could contribute to the 2 deliverables

This was done through the talks and discussion sessions. The slides and some of the videos of the talks are present on the program page (https://europroofnet.github.io/wg3-meeting-timisoara-program/).

Another output of the meeting was a detailed plan on the structure of the 2 deliverables (see sections below).

D5 (month 18): Comparison of the approaches used in the Software Verification competition SV-COMP

- *Contributors*: Dirk Beyer, Ahmed Bhayat, Mădălina Erașcu, Zafer Esen, Carsten Fuhs, Lilia Georgieva, Pamina Georgiou, Wolfram Pfeifer, Mehmet Tahir Sandikkaya, Muhammad Usama Sardar, Jan Tušil
- The deliverable will be a wiki page.
- All output for tool inventory would be nice to follow the format Carsten has proposed in his talk:
    - What inputs are supported?
    - What properties can be verified?
    - What are the tool's main techniques for the supported (input, property) pairs?
    - What external tools are used? (e.g., compilers, SMT solvers)
    - What is the tool's URL?
    - What is the "canonical reference" to a system description?
- Output 1:
    - Tool at invariant generation tools and safety conditions - this is useful for proving termination
    - Inventory of tools for invariant generation and safety conditions starting from Dirk's paper (SV-COMP) and extending it with the tools from the people in the Timisoara meeting
    - Invariant Generation in FramaC (EVA)
- Output 2: Tool overviews for termination: tools in SV-COMP and/or Term Competition
- Output 3: Applications: formal specification and verification of security protocols in emerging and challenging contexts (such as attestation in Confidential Computing)

D6 (month 24): Software prototype for the inference of program specifications as logical axioms.

- *Contributors*: Horațiu Cheval, Amélie Ledein, Dorel Lucanu, Traian Florin Şerbănuţă, Riccardo Treglia, Jan Tušil, Alicia Villanueva
- The deliverable will be a document.

- Output 1: Decide the level of abstraction of specifications: user level (summarization, assert, assume, loop invariant, termination term), tool level (logic-dependent - memory safety, heaps) - listing the possibilities
- Output 2: Technology for inferring the specifications: abstract interpretation, generalisation (overapproximation) of the invariant generation, symbolic execution, case study for abstract interpretation: infer types for Python programs, Dirk's papers on invariant generation and other specifications generation
- Output 3: Technology for validating the generated specifications in the K framework
- Output 4: Liquid Monadic Intersection types in statical analysis of algorithms: Design a type system combining refinement types, the expressiveness of monadic intersection type discipline (where the functor of the monad is a parameter). Prove the subject reduction of the system and develop an inference algorithm, and prove to be sound. Find interesting case studies in which the monad is instantiated and understand how to make the type inference algorithm modular.

Conclusion

The main goals of the event were achieved successfully. As next steps, we have to:

- Set-up the Wiki for D5.
- Create Zulip channels dedicated to the topics of D5 and D6.
- Invite other participants in the action to contribute to D5 and D6.