

WG3 Kick-Off meeting

February 10-11, 2022

WG3 Context

- Several communities/approaches/categories of tools in **program verification**:
 - Theorem provers
 - with expressive type systems as the basis for program verification.
 - to synthesise programs
 - Symbolic representation of state space
 - that use different proof systems to incorporate techniques such as fixpoint reasoning, predicate abstraction, interpolation, backward reachability.
 - Semantic-based approaches
 - inspired on Hoare-based verification, and that use SMT-based reasoning for proving correctness
 - that reduce the verification problem to some kind of logic/constraint representation, that must be solved later by provers
 - semantic frameworks



WG3 Context

Challenge

Formal verification involves solving intractable or even undecidable problems. Techniques and tools require a high level of expertise. This makes it difficult for the industry to embrace formal verification.

- WG3 - beyond the state-of-the-art
 - Verification approaches can envisage **new applications and integration of proof systems** to overcome challenging problems that combine features that are better expressed in different logics.
 - Scalability and usability of verification techniques can be improved thanks to the exploitation of **synergies among different verification tools**.
 - Make verification techniques more successful by **taking advantage of advances on interoperability** between automated and interactive theorem proving, the mathematical formalisation of program semantics, and type theory.



Objectives

Research Coordination Objectives (RCO) for WG3

- Make techniques for program verification more effective and more accessible to all stakeholders.

Capacity-building Objectives (All WG)

- Bring together members of the different communities working on proofs in Europe.
- Act as a stakeholder platform in the field of formal proofs from its theoretical grounds to its industrial applications.
- Create an excellent and inclusive network of researchers in Europe with lasting collaboration beyond the lifetime of the Action.
- Ease access to formal verification techniques in education and other areas of science.
- Actively support young researchers, the under-represented gender, and teams from regions with less capacity.
- Transfer knowledge in terms of expertise, scientific tools and human resources.
- Prepare competitive EU researchers for a fruitful career.
- Disseminate the results of the Action activities.



Implementation

- Each WG: at least one meeting every year to present results and discuss collaborative research activities for the next year.
- Six WGs:
 - WG1 on tools for interoperability.
 - WG2 on automated theorem provers.
 - WG3 on program verification. Tasks:
 - Investigate and develop proof systems for program semantics in cooperation with other working groups;
 - strengthen traditional techniques for program verification;
 - identify and exploit synergies between different verification tools and proof systems;
 - and develop new systems for checking the correctness of programs and complex software.
 - WG4 on libraries of formal proofs.
 - WG5 on machine learning in proofs.
 - WG6 on type theory.



Implementation – First Year

- Goals are agreed for each grant period.
- Directly associated to WG3:
 - Identify verification techniques used in the Software Verification competition SV-COMP and start the analysis and characterization of the different approaches



WG3 deliverables

Stated in the MoU

- **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.
- **D7 (month 48):** Collection of verification challenges with summary of working recipes for verifying them.
- **D8 (month 48):** Technique for syntax-semantics interface for program verification with/without type systems.



Questions?

