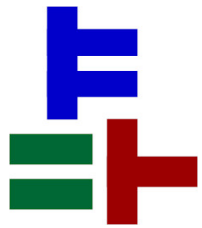
WG3 Deliverables

September 17-19, 2025

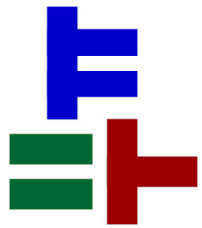
COST is supported
by the Horizon 2020
Framework Programme
of the European Union



WG3 Deliverables

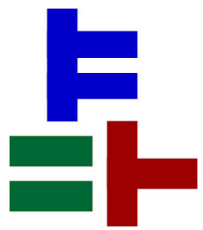
D11. Collection of verification challenges with summary of working recipes for verifying them.

D12. Technique for syntax-semantics interface for program verification with or without type systems.



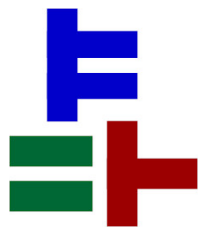
D12 - Syntax-semantics interface for program verification — Type theory

- Roussanka Loukanova: Type-Theory of Algorithms with Chain-Free Memory. DCAI (1) 2024: 65-76
- Roussanka Loukanova: Semantics of Propositional Attitudes in Type-Theory of Algorithms. LENLS 2023: 260-284.
- Roussanka Loukanova: Logic Operators and Quantifiers in Type-Theory of Algorithms. LENLS 2022: 173-198



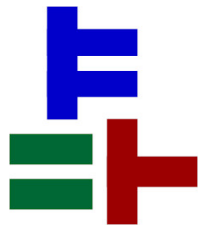
D12 - Syntax-semantics interface for program verification — Rewriting logic

- Maude is a high-performance language and system supporting both equational and rewriting logic computation for a wide range of applications.
- Maude is also a logical framework where other programming languages can be defined (both their syntax and semantics).
- Rewriting logic is reflexive, which is implemented in Maude via a meta-level.



D12 - Syntax-semantics interface for program verification — Rewriting logic

- In this way, we can
  - Define the syntax of a language in Maude (equational part).
  - Define the semantics in Maude (rewriting logic).
  - Execute and analyze programs written in the language defined previously (meta-level).
- Friday talk in MongoDB.

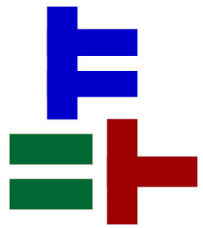


D11 - Verification challenges

- Challenges available in GitHub

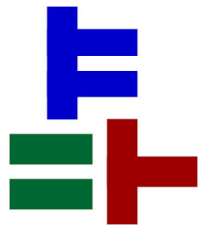
  `https://github.com/EuroProofNet/ProgramVerification/wiki/List-of-challenges`

- We are sure more challenges exist.
- Let's check the ones already proposed.
- One of the relates to a particular technology and the other one to a verification technique.



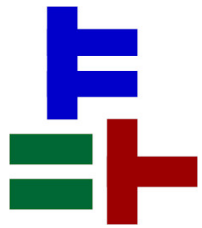
D11 - Verification challenges - TLS

- Challenges related to the Transport Layer Security protocol.
- Thanks to Muhammad Usama Sardar for the contribution as Team lead.
- Two issues described:
  - Issue 1: Incomplete specs (e.g., see here)
  - Issue 2: Vague and outdated specs (e.g., see here)
- As related technology, we emphasize *symbolic security analysis*.



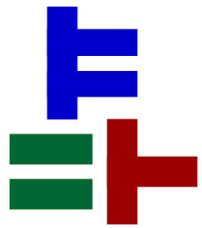
D11 - Verification challenges - Proof scores

- Proof scores are outlines of the formal verification of system properties.
- Proofs are written in the same language as the verification.
- They are a very flexible approach, although they have some formal limitations.
- However, (I consider) they share several issues with “standard” theorem provers.



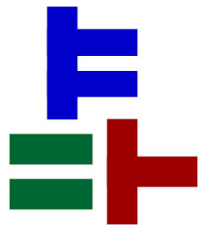
D11 - Verification challenges - Proof scores

- Issues
  - Theorem proving is difficult (only for academia).
  - Theorem proving requires experts (only for academia).
  - There exists a gap between specifications and implementations.
  - Not even theorem proving provides complete assurance (gap!).
  - Theorem proving consumes (too much) resources.
  - Theorem proving is only useful for critical applications.
  - Theorem proving does not work with real problems.



D11 - Verification challenges - Proof scores

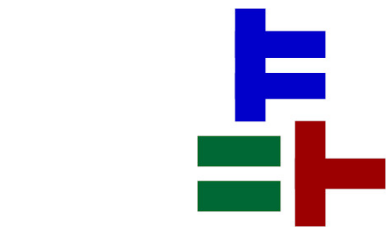
- Solutions(?)
  - Automatizing lemma discovery and proofs.
  - IDE and Graphical User Interface support.
  - Application to New Protocols (previous challenge!).
  - Artificial intelligence support.



D11 - Verification challenges - What we need

- Name of the challenge (used also for the webpage name).
- Short description of the challenge.
- Research team/s involved (or communities).
- Main issues / open problems related to the challenge.
- Techniques and technologies related to the challenge.
- Example(s).
- Other relevant information (external links, references, etc.).
- Status (identified/active/finished/discontinued).

Edit GitHub or send us an email (ariesco@ucm.es and villanue@dsic.upv.es).



Let's discuss and complete the challenges!