WG3 Kick-off meeting

–Report–

WG leaders: Rodica Condurache and Alicia Villanueva

Context

There are many perspectives and approaches to the interaction between proof systems and program verification. The WG3 kick-off 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 Universitat Politècnica de València, in Valencia (Spain). We thank the local organizers for their work and effort that contributed to having a successfull event. One of the main goals was to foster collaborations and to build synergies among participants to ease the path to more fruitful results of the Action.

On the scientific aspect, it contributed to identifying verification techniques used in the Software Verification competition SV-COMP and also other competitions, and starting the analysis and characterization of the different approaches. The identification of verification techniques used in the Software Verification competition SV-COMP was one of the topics discussed during the organized sessions.

Participation and program

The meeting was announced through the official mailing list `epn-wg3-verif@inria.fr`, the Zulip channel (https://epn.zulipchat.com) and on the Action webpage (https://europroofnet.github.io/). Alghough it was initially planned as a face-to-face event, it was held as an hybrid event.

The meeting was attended by 53 researchers in total, 16 of them were on-site participants. Four participants were funded by the action. Most of the participants were members of the action. A few showed their interest in joining the action after the event. The affiliation of the majority of attendees were European universities, but had also the participation of two companies.

The program of this event (shown below) started with the presentation of the COST Action in general and the presentation of the WG3 goals and deliverables. Then, the scientific activity began with a specific talk focused on the first deliverable was given and some short talks were given by COST members. The first day ended with a discussion on topics that could lead to collaborations among COST members and teams. The first session of the second day included short talks and then in small groups participants elaborated on the topics of interest defined during the first day in order to plan future steps.

cost EUROPEAN COOPERATION IN SCIENCE & TECHNOLOGY

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

Day 1	
Opening & Presentation (10:00-10:30):	*The EuroProofNet COST Action and WG3 "Program Verification"* by Frédéric Blanqui, Rodica Condurache, Alicia Villanueva
Deliverables (10:30-11:30): WG3 deliverables	*Comparison of existing tools/benchmarks* by Laura Kovacs
Talks (12:00-13:30)	*Data accounting, Invariants for testing of smart contracts* by M. Gajda *Language-agnostic program verification* by J. Conejero *CPF: The Certification Problem Format* by René Thiemann
Interaction (15:00-16:00):	Identifying goals
Wrapping-up (16:00-17:00):	Conclusion & Plan
Day 2	
Day presentation (10:00-10:20)	
Talks (10:20-11:00)	*Legal certified software through proof assistants: a global scientific and managerial perspective* by J. Joosten *Equational Unification and Symbolic Reachability in Maude* by Santiago Escobar *Converging two directions of program verification: deductive verification meets smart types for smart contracts* by Antonio Ravara
Interaction (11:00-11:30)	
Participants (12:00-13:30):	Towards the deliverables
Wrapping-up (15:00-16:00):	Setting the agenda for the year

Output

One of the outputs of this event has been to allow participants to actively interact among them, building collaborative synergies. The schedule of the meeting reserved time for discussions after each talk that resulted quite fruitful. Thanks to the generosity of the speakers that shared their lines of research, goals and view of the action, the rest of participants had the opportunity to discover common interests.

Regarding the scientific output, first of all, on the meeting webpage the presentations are available. Second, two documents were produced during the meeting:

- the identification of topics of interest (day 1)
- a more specifica plan associated to the identified topics (day 2).

In the following subsection we reproduce, with some annotations and context, these two documents.

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

Topics of interest and plan

The last session of the first day was devoted to identifying topics of interest in the context of the WG3.

To facilitate the discussion, a section with some relevant information extracted from the MoU was provided:

Context:

- Theorem provers as the basis
  - From models/programs to theorem provers
  - Synthesize programs from theorem provers
- Symbolic representation of state space
  - Proof systems to incorporate reasoning/optimization techniques
- Semantic-based approaches
  - Deductive verification
  - Non-standard semantics to reduce the problem to a representation to be checked by proof systems
  - Semantic frameworks such as FramaC or K Framework on top of which verification techniques can be build

Deliverables:

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 types

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.

The first day four topics were identified, and some keywords and description were given for each of them. The four identified topics are

1. Comparison of tools (related to Deliverable 1)
2. Theorem provers as the basis
3. Semantic-based approaches
4. Application domains

Some keywords and initial descriptions were defined during the first day. The goal for the second day was to answer at least some of the more specific proposed questions:

- Can we find a goal for this year?
- Can we find a mid-term or long term goal?
- To which deliverable or action goal would contribute?
- Which can be our the next steps?

During the second part of the second day the participants worked in groups, one for each of the identified topics. Each participant had the possibility to move from one group to another. It was a challenge to have this kind of discussion in an hybrid meeting, but these small discussions were very fruitful as can be seen in the following description of the produced document. We have integrated also information from the description produced during the first day. The small groups resulted also an opportunity to know each other.

The last session of the event served to wrap up. Each group briefly presented the discussed ideas and proposals, which lead to a common knowledge of the action members interests.

Let us know present the description and proposals for each topic. The document was elaborated collaboratively by participants. We thank the coordinators of each topic and all involved participants.

1. Comparison of tools (related to Deliverable 1)

Involved participants: Carsten Fuhs, Michał J Gajda, Laura Kovacs, Rodrigo Raya, Ayşe Sayın, René Thiemann.

Description We can compare several verification-related tools based on different aspects.

- Comparison by using measurable criteria, such as the SV-COMP
- Program level: comparison of tools depending on the programs they can verify
- Reasoning level: comparison of tools depending on the technology used / features
- Model checking (state space). Comparison of model checkers depending on the expressivity of properties verified

- Termination verification. Comparison of termination tools. There is also a competition (Strategies to use termination certificates, e.g. for functional programs, in software verifiers/theorem provers)
- Logical representations from semantic-based approaches. comparison of analysis tools depending on the kind of properties that can be analyzed
- Comparison of domain-specific usability of tools:
  - existing libraries
  - solvability of domain specific constraints/properties

Possible goals for the year

- Get an overview on how different tool competitions are conducted (SV-COMP, TermComp, CoCo, VerifyThis, ...)

  Aspects that can be analyzed:
  - Benchmark design.
  - Performance evaluation.
  - Are the different competitions designed to reflect actual verification needs?
  - What level of trust is required/admissible in each category?
- What are current features / problems? (Both of competitions and tools.)
  - Would tools of one category help with the limitations found in other categories?
  - Can tools of one competition solve problems in other competitions?
  - ...
- Are competitions encouraging advances in the theory of verification?
  - Is there a variety of theoretical foundations within the same category?
  - ...

Outside of competitions, what prominent verification tools are (publicly) available, what inputs and properties can they verify (from a black-box/high-level perspective – the details of hundreds of underlying theorems might (?) be out of scope)? (Facebook Infer, Maude, ...)

A mid-term goal

- Comparison of expressiveness, ease of use...
- Determining tools & competitions list to compare

A corresponding document that addresses some of the goals for this year

- A competition survey.

Associated deliverable or action goal *D5 (month 18): Comparison of the approaches used in the Software Verification competition SV-COMP.*

Next steps

- Create a Zulip sub-channel, invite our team members to it.

2. Theorem provers as the basis

Involved participants: Ana Borges, Juan Conejero, Michał J Gajda, Muharrem Tuncay Gençoğlu, Lilia Georgieva, Mireia González Bedmar, Amélie Ledein.

Description Existing open problems:

- Models to theorem provers:
  - Taking semantics of programming languages from K via Dedukti to some ITPs. Importing the whole semantics of a PL
- Programs to theorem provers:
  - Import K statements to ITPs to reason about programs once we have the model of their PL
  - Exporting property test suites and class declarations as proof obligations (for example Monoid declaration as obligation to prove associativity, QuickCheck property test of `parse . Read == id` as proof that identity holds)
- Synthesize programs

A goal for this year

- Create Zulip Channel for the group discussions
- Meet in about 2 months (tentative: 12 April)

A mid-term goal

- Taking semantics of programming languages from K via Dedukti to some ITPs. Importing the whole semantics of a PL
- Send imported theories from Dedukti to ITPs

Associated deliverable or action goal Initially seems like the following action goals:

1- Express new proof systems in the Dedukti logical framework.

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

Next steps

- Group meeting 12 April (tentative)

3. Semantic-based approaches

Involved participants: Gergely Buday, Rodica Condurache, Michał J. Gajda, Joost J. Joosten, Laura Kovacs, Alicia Villanueva.

Description Existing activities:

- Inference of specifications as logical axioms
  - Target language/domain
  - Kind of specifications
- Synthesis of interactive systems from temporal (LTL?) specifications
- Defining semantics of data analytics summarizations
  - Preservation of "accounting" properties:
    - Sensitivity to all inputs
    - Additivity of the information monoid
    - Completeness of summarization
    - Reverse summarization or "debugging"
  - Defining invariants preserved in financial software:
    - Preservation of money (money or tokens flow between players, does not appear/disappear)
    - Approximated invariants: Verification parameterized by fee rates (for 0.0% rate, there is a specification of lossless exchange, for 5.0% rate we can verify that fee-taker is paid)
  - Model checking of law
    - Adding durations or stopwatches to frameworks like LTL without exploding model checking
    - Experiments with temporal semantics of computational attributes that give best model checking properties
  - Law implementation inside Coq
    - Formal specification of the regulations for tachographs (ER 561/2006)
    - Proving that implementation corresponds to this spec
  - Defining semantics of concurrent functional languages for verification

A goal for this year

- Describing the data analytics summarization on paper.
- Publish model efficient model checking with durations findings
- Verifying DEX contract with respect to the invariants.
- Exchange and interoperability:
  - Check whether data accounting framework can express:
    - Legal fairness: equal treatment of different clients
  - Try using LTL or similar for smart contracts

A mid-term goal

- Workshop on computational semantics of law and regulation (together with Applications)
- Find internship student(s) for industry-academia technology transfer

Associated deliverable or action goal

Next steps

- Interchange of documentations
- Document listing common taxonomy and scope delimitation

4. Application domains

Involved participants: Gergely Buday, Luis Cruz-Filipe, Michał J. Gajda, Ekaterina (Katya) Komendantskaya, Luigi Liquori, Mehmet Tahir Sandıkkaya, Ayşe Sayın.

Description Some application domains were identified during the first day:

- Protocol verification
- Model checking & semantic-based
- AVISPA...
- Verification of Machine learning/AI.

  Main ideas: many specialised tools exist for verification of Neural networks: Some SMT-based (Marabou), some Abstract interpretation based (ERAN). There are some libraries in ITP/Coq (e.g. MLCert). Problems that arise: (a) inter-operability of tools; (b) embedding neural net verification into larger verification projects (complex software has neural nets as components) ; c) scaling verifiers to large neural nets)
- Verification of functional concurrent programs.

  The idea is to develop a verified compiler for a concurrent functional language, experimenting which concurrency features are realisable in a limited time in such a framework. Tool: the HOL4 theorem prover.)
- Verification of financial programs Preservation of value.
- Verification of data analytics and lossless learning. Preservation of information, proving sensitivity and completeness of summarization
- Verification of smart contracts Not all overlap with financial software

A goal for this year

- Discuss the common problems/challenges across the application areas, e.g.
- Formulate benchmarks for different problems, and try to find grounds for comparison
- Perhaps comparison of languages and provers used in each domain? (Coq, HOL, Tamrin, domain-specific, Agda; Imandra)

A mid-term or long term goal Potential joint research topics:

1. Joint work on verification of concurrency + protocols?
2. Joint problem across AI and Security: components of systems are delegated to NNs or ML; challenge to verify black boxes (?) and then embed that into the standard verification cycle.
3. Linking to groups that formalise law applicable in these application domains, and see to extend their methods to Security, AI, smart contracts...
    - Layers of work in formalisation of legal systems and law:
        - Work on semantics of legal connectives, and commonly used legal constructs (like "fair to all customers")
        - Work on formalisation of specific, narrow regulations (like tachographs, or immigration law decisions)
        - Work on semantic connection within a whole body of law – does not need to be consistent, mostly ML approaches.
4. Protocols (e.g. Networks, Contact Tracing, IoT, etc) can be good application domains for putting current and future Proof Assistants (PA) @ work.

Associated deliverable or action goal

D1. Application dimension to tool comparison

D3. Collection of verification challenges, from the applications perspective (each application domain we listed is itself a challenge for the community)

Next steps

- Create a Zulip sub-channel, invite our team members to it. Invite other key players in verification of these applications
- Make connections with all subgroups of WG3, to understand better the current landscape of law formalization: tools, application areas, ...
- Come up with concrete ideas for collaboration

Finally, let us mention and thank again the contributors to the document: Juan Conejero, Michał J Gajda, Joost J. Joosten, Mireia González Bedmar, Carsten Fuhs, Luigi Liquori, Mehmet Tahir Sandıkkaya, Rodrigo Raya, René Thiemann and Ekaterina Komendantskaya.

cost EUROPEAN COOPERATION IN SCIENCE & TECHNOLOGY
COST is supported by the Horizon 2020 Framework Programme of the European Union

Conclusion

The main goals of the event were achieved successfully. The number of participants was bigger than expected, probably thanks to the hybrid modality for the event. We think that this was a step towards building network of researchers that eases to reach the action goals. At the end of the meeting, we have some ideas for next steps and possible collaborations. Finally, we are grateful to all the speakers that shared their expertise and knowledge with the participants.

We thank the Action Management Committee for letting us have this WG3 kick-off meeting, all the participants and the local organization.

A List of participants

- María Alpuente (UPV - Spain)
- Damián Aparicio-Sánchez (UPV - Spain)
- Frédéric Blanqui (INRIA - France)
- Ana Borges (Universitat de Barcelona - Spain)
- Gergely Buday (Institute of Technology - Hungary)
- Laura Castro (University of A Coruña - Spain)
- Rodica Condurache ("A.I.Cuza" University of Iasi - Romania)
- Juan José Conejero-Rodríguez (Runtime Verification Inc. - USA)
- Luís Cruz-Filipe (University of Southern Denmark - Denmark)
- Ugo de'Liguoro (Università di Torino - Italy)
- Madalina Erascu (West University of Timisoara - Romania)
- Santiago Escobar (UPV - Spain)
- Thiago Felicissimo (INRIA - France)
- Maribel Fernandez (King's College London - UK)
- Pascal Fontaine (University of Liège - Belgium)
- Carsten Fuhs (University of London - UK)
- Michał Gajda (Migamake - Singapore)
- Emilio Jesus Gallego-Arias (INRIA - France)
- Muharrem Tuncay Gencoglu (Firat University - Turkey)
- Lilia Georgieva (Heriot-Watt University - UK)
- Vaidas Giedrimas (Siauliai University - Lithuania)
- Tobias Gleißner (Freie Universität Berlin - Germany)
- Mireia González-Bedmar (Formal Vindications S.L. - Spain)
- Candelaria Hernández-Goya (Universidad de La Laguna - Spain)
- Kuen-Bang Hou-Favonia (University of Minnesota - USA)
- Joost Joosten (Universitat de Barcelona - Spain)

- Ekaterina Komendantskaya (Heriot-Watt University - UK)
- Laura Kovacs (Vienna University of Technology - Austria)
- Julia Lawall (INRIA - France)
- Amélie Ledein (INRIA - France)
- Luigi Liquori (INRIA - France)
- Raúl López-Rueda (UPV - Spain)
- Dorel Lucanu (Alexandru Ioan Cuza University - Romania)
- Salvador Lucas (UPV - Spain)
- Fatih Ozkaynak (Firat University - Turkey)
- Sergio Pérez Rubio (UPV - Spain)
- António Ravara (Universidade Nova de Lisboa - Portugal)
- Rodrigo Raya (EPFL - Switzerland)
- Adrián Riesco (Universidad Complutense de Madrid - Spain)
- Mehmet Tahir Sandikkaya (Istanbul Technical University - Turkey)
- Julia Sapiña (UPV - Spain)
- Ayse Sayın (Istanbul Technical University - Turkey)
- Josep Silva (UPV - Spain)
- Volker Stolz (University of Oslo - Norway)
- Geoff Sutcliffe (University of Miami - USA)
- Rene Thiemann (University of Innsbruck - Austria)
- Amin Timany (Aarhus University - Denmark)
- Dmitriy Traytel (University of Copenhagen - Denmark)
- Shmuel Tyszberowicz (The Academic College of Tel-Aviv Yaffo - Israel)
- German Vidal (UPV - Spain)
- Alicia Villanueva (UPV - Spain)
- Chuangjie Xu (fortiss - Germany)