Minutes of PARDI second Paris meeting

20th december 2017

The purpose of this report is to keep track of the questions and discussions which occurred during the meeting. Refer to the slides for more details on the presentations.

Participants

Sylvain Conchon, Mamoun Filali, Aurélie Hurault, Stephan Merz, Meriem Ouederni, Pascal Poizat, Philippe Quéinnec, Fatiha Zaïdi.

Content

Progress report on Pardi (Philippe)

A progress report at the end of the first year of Pardi is presented. The main initial deliverables are on time. Several evolutions for the next deliverables are discussed:

- In task 2 (automatic verification of parameterized systems), an early deliverable is "Cubicle that can take as input TLA+ programs". It appears that the input language of Cubicle is directly linked to its data structures and its expressiveness: it is useless to understand all TLA+ if Cubicle cannot prove anything on the formulae. As we already have a translator from (a subset of) TLA+ to Cubicle, we have decided to postpone this deliverable until Cubicle has improved its expressiveness.
  Work on Cubicle is ongoing on counters (Mattias Roux) and on invariants inference (David Declerck).
- In task 3 (mechanized proofs of parameterized systems), the architecture for interaction between model checker and proof assistant is discussed (see below). Note that one of the deliverable far in the future ("TLA+ library for communication" at T0+36) has greatly progressed and work on fault models is ongoing.
- In task 4 (automatic verification of parameterized workflow systems), the need for a new DSL is reconsidered. Work has greatly progressed on defining the semantics of parameterized BPMN collaborations (see below).

Staff

- First PhD recruitment: Adam Shimi at Toulouse INP/IRIT (September 2017)
- Second PhD recruitment: Sarah Hourou at UPMC/LIP6 (January 2018)
- Launch of Post-doc recruitment at INRIA Nancy - Grand Est

Verification of two wait-free algorithms (Aurélie)

Presentation of the proof of the splitter (see case studies) in Why3. This requires the statement of lots of small invariants which are combined to prove the splitter. The splitter has also been modeled in Cubicle but the expected properties are not checkable (they require existential quantification). The proof of the renaming (see case studies) in Why3 is incomplete. There is no cubicle model for the renaming as it requires arithmetic operations on the process id.

Semantics of parameterized BPMN collaborations (Pascal)

Work has progressed on defining the semantics of parameterized BPMN collaborations in a way that makes it amenable to a TLA+ specification (Sarah Hourou and Pascal Poizat). A new case study (e-publishing) is added to the repository.

Formal semantics of parameterized BPMN collaboration is presented. It is parameterized both on the number of instances and on the properties of message delivery (when is a message available?). FOL is used to express the semantics and it looks close to TLA+ predicates. It seems reasonable to specify the model engine in TLA+. Discussion on the properties that will be verified: blocking in a process, termination with an empty network.

Interactions between the automatic discovery of invariants and a proof assistant (discussion leaded by Sylvain)

The manual or assisted proof of an invariant generally requires proving lots of small invariants. Identifying these invariants and proving them is often tedious. This task proposes the following method:

1. Fix the values of the parameters (for instance the number of processes).
2. Check by automated verification (Cubicle or DVF) the main goal. As the parameters are fixed, the goal and its verification should pass.
3. Examine the invariants which are found during the verification, and generalize them (for instance by removing the explicit values of the parameters).
4. Relaunch the automated verification on these generalized invariants to prove them.
5. Use these invariants to prove the main goal in TLAPS or Why3. As these invariants were discovered while proving the main goal with fixed parameters, they are expected to be useful and/or necessary.

Incoming Actions

- Next meeting in May in Nancy.
- Inspection on the licence of Intel DVF tool (Sylvain)
- e-publishing workflow in TLA+ (Aurélie, Philippe).
- TLA+ specification of the BPMN workflow engine based on Pascal's semantics (Pascal, Philippe).
- Experiments with the TLA+ to Cubicle translator (Stephan, Philippe)