Minutes of PARDI first Paris meeting

11th july 2017

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

Participants

Souheib Baarir, Sylvain Conchon, David Declerck, Lom Hillah, Aurélie Hurault, Alain Mebsout, Stephan Merz, Pascal Poizat, Philippe Quéinnec, Mattias Roux, Fatiha Zaïdi.

Content

Progress on Cubicle "classic" (Alain Mebsout)

New version of Cubicle (1.1.1)

- Murphi (an explicit model-checker) is used as an oracle for the enumerative forward pass. It helps in finding invariants used in backward reachability.
- Language extensions: macros, new logical operators
- L. Matthews et al. "Verifiable Hierarchical Protocols with Network Invariants on Parametric Systems", FMCAD 2016
- Documentation is to come.

Progress on Cubicle with weak variables (David Declerck)

Cubicle with weak variables.

- TSO semantics for weak variables
- Fence to force consistency
- Axiomatic memory model: reads and writes generate events. Events are ordered according to several partial orders (e.g. total order in a process, a reading of a value occurs after the writing of this value, etc). This yields an happened-before relation, which must be acyclic (linearisable) for the execution to be possible.
- Currently, no invariant generation including a weak variable.
- Can this approach be adapted to other memory models? Not done, but seems possible.
- This is close to message sending and receiving, and to partial orders in distributed algorithms. It seems reasonable to adapt this approach to channels (FIFO).
- Shared memory seems closer to broadcast communication (one writer, and a set of reader) than to point-to-point communication (where the receiver consumes the message, making it unavailable for other processes).

Cubicle: forward abstracted reachability (Mattias Roux)

- How to build an inductive invariant, by strengthening an initial invariant with the preimage of the bad states.
- Backward reachability with set cardinality `#{p. crit[p] = True} > 1`

Translation TLA+ to Cubicle (Stephan Merz)

Translation of a fragment of TLA+ into Cubicle language.

- Translation of the fragment of TLA+ which is the closest to Cubicle.
- Safety only as Cubicle does not check liveness.
- Use a standardized type invariant to generate Cubicle declarations.
- Support enumerative types (set of strings in TLA+), boolean, int and array of processes.
- TLA+ actions with a standard form (`Act(i) == guard /\ x' = e /\ ...`) are translated in Cubicle transitions.
- Array support obviously translates `[ x EXCEPT ![p] = e ]` into Cubicle corresponding syntax.
- Currently rather preliminary (and not necessarily an important objective of Pardi), but could ease the writing of examples.
- Cubicle counter-examples are not translated back as a TLA+ traces, but the translation is close enough and it should be possible (not an objective).
- Available on github.

Case studies and Parameters (Philippe Quéinnec)

- Presentation of the available case studies
- Analysis of the parameters used in these examples
- Details in deliverables D1.1 and D1.2
- New framework for the verification of communicating peers

Progress on workflow models (Pascal Poizat)

- BPMN verification is mainly concerned with behavioral models and uses ad-hoc translation to Petri nets, LTS,...
- Trend: control flow (BPMN) + data
- Objective: give FOL semantics for BPMN, then translate to SMT-lib, TLA+, Cubicle. Discussions on the choice of SMT-lib, why not prefer a richer tool with existing libraries for advanced data structure (e.g. why3)?
- Case studies:
  - Expand the Exam Management System to include multiple students and professors.
  - New: an eConference system (e.g. a simplified version of easychair).
    - a data model is required.
    - multiple processes can be realized by the same human user.
    - data-related numerical parameters: e.g. every paper is reviewed by n1 to n2 reviewers.

- Questions:
  - Communication parameters? Topologies?
  - Distributed algorithms as choreographies?
  - Parameters for external services?

Deliverables

- D1.1 Case studies: see repository.
- D1.2 Report on the case studies and the considered parameters (also in the repository).

Incoming Actions

- Next meeting in November at Paris Saclay.
- Initial definition of a parametric WF DSML (workflow domain-specific modeling language) at t0+12 (first version). This corresponds do the first iteration of deliverable D4.1.
- Principles of interaction between an interactive theorem prover and a model checker (deliverable D3.1).