2018-00673 - PhD Position: Checking TLA+ Invariants by Finite Model Finding [S]

Contexte et atouts du poste

TLA* is a general-purpose language that has found applications in formal specification of distributed systems. In the last years, the developers of the TLA* tools made significant progress towards automation of the proof system for TLA* [1]. Since writing proofs is an ingenuous task, TLA* users debug their specifications with the TLC model checker [2] before investing significant efforts into writing formal and complete proofs. TLC enumerates reachable states and thus rapidly exhausts all available computer resources.

Recently, we have started to develop a symbolic model checker for TLA* [3, 4] that builds upon two successful approaches to verification: (1) bounded model checking (BMC), and (2) satisfiability modulo theory (SMT). In our current approach, similar to TLC, the user has to define the values of all parameters. Hence, although our model checker benefits from using symbolic techniques, verification is restricted to fixed parameter values, and one has to try several instances in order to get some confidence in the safety of the system.

Mission confiée

In this project, we propose to develop a technique for invariant checking of TLA* specifications that would require the user to give an upper bound on the parameters and variables that constitute a system state, rather than precisely fixing parameter values. For instance, one could bound the values of the integer variables, cardinality of the sets, and cardinality of the function domains and codomains. Given such an upper bound, the technique will produce an SMT encoding of the invariant checking problem, which uses only decidable theories. If an invariant candidate Inv violates one of the proof obligations Init \(\rightleftharpoons\) Inv or Inv \(\land\) Next \(\rightleftharpoons\) Inv’ for some parameters within the provided bounds, the SMT solver should report satisfiability of the problem and give the user a counterexample to the invariance of Inv. Otherwise, the SMT solver should report unsatisfiability, which will guarantee system safety within the provided bounds.

Principales activités

To solve the problem, one will have to answer the following questions:

1. Which metrics should one use in order to bound variable values? Clearly, for an integer variable, one can use the value of the variable. It is less obvious which metric one should use for sets of sets or for functions of TLA*.

2. How to automatically find reasonable bounds on the values of individual variables, given a few bounds from the user? Given two different integer variables in a TLA* specification, the range of their values in an execution may significantly differ. Thus, using a uniform bound for all the variables may be inefficient.

3. Which SMT encoding would work best for this problem? In practice, performance of an SMT solver may dramatically improve, when one carefully chooses an encoding of the problem in SMT. Thus, one has to experiment with various encodings of TLA*.

4. Is the approach able to detect bugs in practical TLA* specifications? We propose to evaluate applicability of the technique by checking safety of fault-tolerant distributed algorithms.

This research involves the development of a new technique and of a prototype implementation. As an extended research beyond the proposed problem, the student can investigate how to leverage the technique to parameterized model checking or to strengthen the invariant when a counter-example is found. The first extension would allow users to check invariants for sets of instances where bounds are not fixed for some variables of the specification. The second extension would reduce the number of spurious counter-examples reported by the model checker.


Compétences
We expect the candidate to be familiar with the following subjects:

- Solid background on formal logic and verification techniques, in particular model checking and/or theorem proving or SMT solving.
- Solid programming experience, preferably in a functional language.
- Prior knowledge of TLA⁺ or a similar set-based specification language is a plus, but is not required.

The candidate should appreciate working on both fundamental aspects and the validation by a prototypical implementation. The working language is English.

Avantages sociaux
- Subsidised catering service
- Partially-reimbursed public transport
- Social security
- Paid leave
- French courses

Rémunération

Monthly salary after taxes: around 1596,05€ for 1st and 2nd year. 1678,99€ for 3rd year. (medical insurance included).