2018-00866 - Temporary Research Position / Software engineering / Proofs and Verification

Contract type : Public service fixed-term contract
Level of qualifications required : PhD or equivalent
Fonction : Temporary Research Position

Context

Research team: Tools for Proofs, MSR-INRIA Joint Centre

The Microsoft Research-INRIA Joint Centre is offering a 24-month position for a research engineer to contribute to the design and further development of the TLA+ Proof System (TLAPS), http://msr-inria.com/projects/tools-for-proofs).

Research Context

TLA+ is a language for specifying and reasoning about systems, including concurrent and distributed systems. It is based on first-order logic, set theory, and temporal logic. TLA+ and its tools have been used in industry for more than a decade. More recently, we have extended TLA+ by a language for writing structured formal proofs and have developed TLAPS, a proof checker that contains an interpreter for the proof language and interfaces with different back-end provers, including SMT solvers, the tableau prover Zenon that supports set-theoretic constructions, and a declarative encoding of TLA+ set theory as an object logic in the logical framework Isabelle. TLAPS is integrated into the TLA+ Toolbox, an IDE for TLA+ (http://lamport.azurewebsites.net/TLA/tla.html).

Although it is still under active development, TLAPS is already quite powerful and has been used for several verification projects, in particular in the realm of distributed algorithms (e.g., http://lamport.azurewebsites.net/TLA/asyncpaxos.html).

The current version of TLAPS handles the “action” part of TLA+: first-order formulas with primed and unprimed variables that represent the values of a variable before and after a transition. It also supports the propositional fragment of temporal logic. This fragment is enough for proving safety properties (invariants and step simulation). We have initiated a complete rewrite of the code base, with the aim of providing support for module instantiation and for the full temporal logic of TLA+, which will allow us to prove liveness and refinement properties.

Assignment

Description of the activity of the research engineer

The research engineer (post-doctoral) position is funded for 24 months by the Microsoft Research - INRIA Joint Centre. You will work together with the members of the TLA+ project, including Damien Doligez, Leslie Lamport, and Stephan Merz on extending the TLA+ Proof System. Your main objective will be to complete the rewrite of the existing version of TLAPS so that it can be released to users of the prover. You will also be able to work on extensions of existing functionality, including the following items:

- Module instantiation. The TLA+ language contains a module system, and modules can have constant and variable parameters in order to make them generic and reusable. When a module is instantiated, parameters can be replaced by constant- and state-level expressions, and these instantiations must be taken into account when generating proof obligations for back-end provers.

- Handling temporal logic. Proofs of liveness properties need support for reasoning about first-order temporal logic, such as induction over well-founded orderings. Fairness hypotheses require reasoning over the enabledness of actions. New backend provers need to be set up and integrated into TLAPS for carrying out these proofs.

- Improved backend provers. The current backend provers provide decent support for proof obligations mixing first-order logic, elementary set theory, functions, and integer arithmetic. Reasoning about other important data structures such as finite sequences requires low-level user interaction. We are interested in exploiting advances in automatic deduction techniques, such as support for relevant theories in SMT solvers, for enabling a higher degree of automation of such proof steps.

- Rigorous validation of soundness. Computing proof obligations involves some subtle transformations, such as distributing the prime operator of TLA+ or handling instantiated ENABLED expressions. We are working on a precise definition of the semantics of the proof language that would help us ensure the soundness of these transformations and give guidelines to the implementors.

General Information

- Theme/Domain : Proofs and Verification
  Software engineering (BAP E)
- Town/city : Paris
- Inria Center : CRI de Paris
- Starting date : 2018-09-01
- Duration of contract : 2 years
- Deadline to apply : 2018-07-31

Contacts

- Inria Team : GALLIUM
- Recruiter : Damien Doligez / damien.doligez@inria.fr

About Inria

Inria, the French National Institute for computer science and applied mathematics, promotes "scientific excellence for technology transfer and society". Graduates from the world’s top universities, Inria’s 2,700 employees rise to the challenges of digital sciences. With its open, agile model, Inria is able to explore original approaches with its partners in industry and academia and provide an efficient response to the multidisciplinary and application challenges of the digital transformation. Inria is the source of many innovations that add value and create jobs.

The keys to success

Skills and profile of the candidate

You should hold a PhD degree in computer science and have solid knowledge of mathematical logic, as well as implementation skills related to symbolic theorem proving. TLAPS is mainly implemented in OCaml, but some Java programming will be necessary for interfacing TLAPS with the other TLA+ tools. Experience with temporal and modal logics, with interactive theorem provers or with Eclipse could be valuable.

Work on TLAPS provides the opportunity to learn about issues of using deductive verification in practice, and there are possibilities to produce publishable research. However, the main focus is on the implementation of components of our tool chain that are missing or need improvement.

Given the geographical distribution of the members of the team, we highly value a good balance between the ability to work in a team and the capacity to propose initiatives.

Conditions for application

Defence Security:
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST). Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy:
As part of its diversity policy, all Inria positions are accessible to people with disabilities.
- Checking SMT proofs. The SMT backend handles most of the proof obligations that occur in practice. The current version of TLAPS assumes the external SMT solver to be correct, but we are interested in reconstructing proofs provided by SMT solvers within Isabelle/TLA+. The Zenon backend already benefits from proof reconstruction.

- Performance issues. Proof projects can be large, and TLAPS implements mechanisms, such as fingerprinting proof obligations, that are intended to make the tool scale. Performance bottlenecks should be monitored and avoided, whenever possible.

- Case studies and proof libraries. Our work on TLAPS is validated by carrying out case studies, and we provide libraries of lemmas that are useful for many proof projects.

We do not expect to be able to address all of these issues within 24 months. The choice of items will be made jointly with the research engineer, also depending on his or her interests and background.

Main activities

Main activities:
- Design and development of extensions of the TLA+ Proof Manager.

Additional activities:
- Maintenance of the TLA+ Proof Manager
- Documentation
- Case studies

Skills

Technical skills and level required: programming, proofs in formal logic, design of formal logics

Languages: TLA+, Java, OCaml

Relational skills: autonomy and long-distance communications

Benefits package

- Subsidised catering service
- Partially-reimbursed public transport

Remuneration

Poste localisé Paris 12ème.

Rémunération selon profil et expérience.