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 TLAPS tool chain that are missing or need improvement. The main focus is on the possibilities to produce publishable results on TLA+. However, the main focus is on the implementation of components of our tool chain that are missing or need improvement.

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 automated proving is an advantage. TLAPS handles the “action” part of TLA+ first-order formulas; it can handle both 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). However, the main focus is on the implementation of components of our tool chain that are missing or need improvement.

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). Authorization 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.