We do not expect to be able to address all of these issues within 24 months. The Doligez, Leslie Lamport, and Stephan Merz on extending the TLA+ Proof System. will work together with the members of the TLA+ project, including Damien Principales activités refinement. prove liveness and refinement properties, has been implemented, but requires further the full temporal logic of TLA+, which will allow us to fragment of temporal logic. This fragment is enough for proving safety variable before and after a transition. It also supports the propositional formulas with primed and unprimed variables that represent the values of a variable. 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). Preliminary support for the full temporal logic of TLA+, which will allow us to prove liveness and refinement properties, has been implemented, but requires further refinement.

Principales activités
The contractual researcher (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 provide full support for temporal reasoning in 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.
- 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 implementation.
- 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 researcher, also depending on his or her interests and background.

**Compétences**

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.

**Avantages**

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking (after 6 months of employment) and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

**Rémunération**

From 2632 euros gross monthly (according to degree and experience)

---

**Attention:** Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.