Offre n°2022-04909

PhD Position F/M Formalization of Set Theory and Proof Checking

Le descriptif de l'offre ci-dessous est en Anglais

Type de contrat : CDD

Niveau de diplôme exigé : Bac + 5 ou équivalent

Fonction : Doctorant

Contexte et atouts du poste

Team
VeriDis, Inria Nancy Grand-Est, https://team.inria.fr/veridis/

Contact
Stephan Merz (stephan.merz@loria.fr)

This PhD position is funded by the ANR project ICSPA (Interoperable and Confident Set-based Proof Assistants).

Mission confiée

Context

The B, Event-B, and TLA+ methods are well-known formalisms that target the development of software systems used in critical applications, subject to stringent certification requirements. Mathematically, they are based on variants of Zermelo-Fraenkel set theory, and their application generates proof obligations, for example for ensuring the preservation of invariants or the correctness of refinements between models described at different levels of abstraction. All three methods are supported by toolsets (Atelier B, Rodin, and the TLA+ Toolbox) that include trusted engines for automatic proof and implement translations from the set-theoretic language underlying the methods to the input languages of automatic theorem provers.

The ANR project ICSPA aims at improving confidence in the proofs carried out in the context of B, Event-B, and TLA+ by formally and independently verifying these proofs using an independent proof checker with a small trusted base. Moreover, given the similarity between the underlying mathematical theories of these methods, it aims at enabling sharing and reusing proofs and theories between B, Event-B, and TLA+. Both objectives rely on the use of a common logical framework, called the $\Lambda\Pi$-calculus modulo theory and implemented in the system Dedukti, in which any formal proof system can be expressed.

ICSPA brings together academic experts in formal methods and deductive reasoning (Samovar, Inria Nancy, Inria Saclay, IRIT, and LIRMM) and the Clearsy company, a leader in the application of formal methods to the design of critical systems, in a 4-year effort that aims to increase confidence and reuse of theories and proofs.

Principales activités

Project description

The first objective of the thesis is to express TLA+ set theory and proofs in the $\Lambda\Pi$-calculus modulo theory and implement it in Dedukti, in a way that enables interoperability with the set theory of B and Event-B. In particular, the logic of TLA+ is untyped whereas B and Event-B are based on a typed logic. It is therefore expected that it will only be possible to define partial translations between the two formalisms, exploiting the fact that many proofs do not use the full power of the theory they are expressed in. The representation of TLA+ set theory can reuse ideas from the existing encoding in the logical framework Isabelle for TLAPS, the TLA+ Proof System.

In a second step, the back-end proof engines of TLAPS have to be instrumented in order to export proofs for checking by Dedukti. A similar mechanism has already been implemented for checking proofs produced by the Zenon back-end in Isabelle, but it will be adapted for Dedukti and extended to the proof traces provided by SMT solvers such as veriT and CVC5.

Finally, the thesis will study the export to Dedukti of full TLA+ specifications, rather than just individual formulas as for proof obligations, as well as the import of transition systems represented in Dedukti, in particular those arising from the translations from B and Event-B models. The purpose of these translations is to achieve reuse of (parts of) specifications expressed in B, Event-B, and TLA+, including importing libraries without having to reprove the associated theorems.

The thesis will be carried out at the Inria research center in Nancy, France, in joint supervision with Gilles Dowek from Inria Saclay, and in close collaboration with the partners of the BLaSST project that focus on the B and Event-B methods. The expected starting date is September 1 or October 1, 2022, but a later starting date can be agreed upon.

Compétences

Required qualifications

The candidate must hold (or be about to obtain) a Master degree in computer science. Candidates must have solid knowledge in mathematical logic and preferably in automated or interactive reasoning. Experience with formal methods such as B, Alloy, TLA+ or Z would be a plus. The candidate should be fluent in a mainstream programming language such as OCaml, C++ or Java.

Language

English or French.

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

Salary: 1982€ gross/month for 1st and 2nd year. 2085€ gross/month for 3rd year.

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

Informations générales

- **Thème/Domaine :** Preuves et vérification
- **Ville :** Villers lès Nancy
- **Centre Inria :** Centre Inria de l'Université de Lorraine
- **Date de prise de fonction souhaitée :** 2022-10-01
- **Durée de contrat :** 3 ans
- **Date limite pour postuler :** 2022-11-30

Contacts

- **Équipe Inria :** VERIDIS
- **Directeur de thèse :**
  Merz Stephan / Stephan.Merz@loria.fr

A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines. L'institut fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. 900 personnels d'appui à la recherche et à l'innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 200 start-up. L'institut s'efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

L'essentiel pour réussir

Application deadline

June 30, 2022 (midnight Paris time)

How to apply

Upload your application on jobs.inria.fr in a single pdf or zip file, and also send it by email to stephan.merz@loria.fr. Your file should contain the following documents:
· Your CV.
· A cover/motivation letter describing your interest in this topic.

· A short (max one page) description of your Master thesis (or equivalent) or of the work in progress if not yet completed.
· Your degree certificates and transcripts for Bachelor and Master (or the last 5 years).
· Master thesis (or equivalent) if it is already completed and publications if any (it is not expected that you have any). Only the web links to these documents are preferable, if possible.

In addition, one recommendation letter from the person who supervises(d) your Master thesis (or research project or internship) should be sent directly by his/her author to stephan.merz@loria.fr.

Applications are to be sent as soon as possible. Informal enquiries about the position are welcome by email to stephan.merz@loria.fr and gilles.dowek@inria.fr.

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.

Consignes pour postuler

Sécurité défense :
Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini dans l'arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l'annulation du recrutement.

Politique de recrutement :
Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.