Offer #2022-04898

PhD Position F/M Automated Reasoning for Set Theory

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

Context

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

Contacts
Stephan Merz (stephan.merz@loria.fr) and Sophie Tourret (sophie.tourret@loria.fr)

This PhD position is funded by the ANR project BLaSST (Enhancing B Reasoners with SAT and SMT Techniques).

Assignment

Context

The B method is a formalism based on set theory that targets the development of software systems used in critical applications, subject to stringent certification requirements. It defines proof obligations that ensure the preservation of invariants or the correctness of refinements between models described at different levels of abstraction, and these proof obligations must be discharged for a model to be accepted as valid.

The application of the B method is supported by Atelier B, maintained by the Clearsy company, a platform that contains several engines for automatic proof. In a recent experiment, among the roughly 77,000 proof obligations of a representative industrial development project, 64% were proved automatically, leaving 28,000 obligations to be proved by human interaction. Also, no significant feedback is provided in case an obligation cannot be proved. Given recent advances in automated theorem proving, we believe that the number of proof obligations that can be discharged automatically can be improved significantly, and that tools can help users by explaining why certain obligations cannot be proved.

The ANR project BLaSST aims at bridging combinatorial and symbolic techniques in automatic theorem proving, in particular for proof obligations arising from models written in the B formalism. Work will be carried out on SAT-based techniques as well as on more expressive SMT formalisms. In both cases, encoding techniques, optimized resolution techniques, model generation, and lemma suggestion will be considered. Combining both lines of work, the expected scientific impact is a substantially higher degree of automation of solvers for expressive input languages by leveraging higher-order reasoning and enumerative instantiation over finite domains. The effectiveness of the techniques developed in the project will be evaluated by applying them to benchmark sets provided by the industrial partner.

BLaSST brings together academic experts in automated reasoning techniques (CRIL, Inria Nancy, and the University of Liège) 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 provide a breakthrough in formal verification applied to software design.

Main activities

Project description

Automated deduction has made significant progress in recent years, including the development of efficient SAT and SMT solvers, and the extension of first-order deduction techniques to fragments of higher-order logic.

The core objective of the thesis is to make these advancements available for system developments in the B method. Concretely, we believe that higher-order logic allows for a much more direct encoding of proof obligations expressed in a language of set theory than existing translations to first-order logic. This should be beneficial for developing specific instantiation techniques that can recognize frequent patterns that arise in B specifications, significantly raising the degree of automation.

A second objective of the thesis is the design of techniques for constructing counter-models in order to

provide feedback when a proof fails. Since B models written for industrial developments often contain restrictions to finite-state domains, a stronger integration of SAT solving, beyond just handling the propositional structure of formulas, appears to be beneficial for this objective, as well as for proofs by enumeration.

The thesis will be carried out at the Inria research center in Nancy, France, in close collaboration with the partners of the BLaSST project. The expected starting date is September 1 or October 1, 2022, but a later starting date can be agreed upon.

Skills

Required qualifications

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

Language

English or French

Benefits package

- 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

Remuneration

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

General Information

- **Theme/Domain :** Proofs and Verification
- **Town/city :** Villers lès Nancy
- **Inria Center :** Centre Inria de l'Université de Lorraine
- **Starting date :** 2022-10-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2023-01-31

Contacts

- **Inria Team :** VERIDIS
- **PhD Supervisor :**
  Merz Stephan / Stephan.Merz@loria.fr

About Inria

Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and entrepreneurial projects that have a worldwide impact.

The keys to success

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 send it as well 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 sophie.tourret@loria.fr.

Warning : you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.

Instruction to apply

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.