Offer #2025-08765

Post-Doctoral Research Visit F/M Bridging the gap between a safe programming language and a formal proof

Contract type : Fixed-term contract

Level of qualifications required : PhD or equivalent

Fonction : Post-Doctoral Research Visit

About the research centre or Inria department

The Inria research centre in Lyon is the 9th Inria research centre, formally created in January 2022. It brings together approximately 300 people in 16 research teams and research support services.

Its staff are distributed at this stage on 2 campuses: in Villeurbanne La Doua (Centre / INSA Lyon / UCBL) on the one hand, and Lyon Gerland (ENS de Lyon) on the other.

The Lyon centre is active in the fields of software, distributed and high-performance computing, embedded systems, quantum computing and privacy in the digital world, but also in digital health and computational biology.

Context

One of the long-term goals of the ERC project Fresco is to turn the Coq proof assistant into a competitive tool for doing verified computer algebra. In particular, this requires the ability to implement and formally verify well-known libraries such as GMP or BLAS/LAPACK. A significant milestone was the design of Capla, a safe

low-level imperative language suitable for implementing such algorithms, as well as the development of a formally verified compiler for this language.

This postdoc will take place at the LIP Computer Science laboratory of ÉNS Lyon, in the Inria team Pascaline, which aims at advancing the fields of computer arithmetic and computer algebra, with a strong accent on formal verification.

Assignment

It is now possible to write a library using Capla, to compile it to machine code, to verify its correctness using Coq, and to invoke its functions from C code. But to turn the Coq proof assistant into a usable computer algebra system, one should also be able to execute such Capla functions from a Coq script. Moreover, one should be able to use the resulting values inside a Coq proof. The goal of this postdoc is to research and implement a bridge between the proof assistant and a user library written in Capla.

Main activities

The first objective of this postdoc is to provide a way to effectively interface the Coq kernel with Capla code. This requires to tackle several challenges:

- devise a representation of Capla values (i.e., machine integers, multi-dimensional arrays) as Coq terms, and conversely (beware of open terms);
- devise a way to represent Capla computations as Coq terms (e.g., functions, relations, monads, etc), as well as a way to associate some useful yet consistent semantics to these terms (beware of termination issues);
- modify Coq so that it can effectively perform these computations, i.e., convert the input Coq values to Capla, execute the corresponding compiled code, and convert the result back.

The second objective is to make it simpler to formally verify Capla functions. Again, this requires to tackle several challenges:

- devise a semantics that is better suited for deductive program verification than the current operational small-steps one;
- devise a program logic that leverages the features of the Capla language, especially its absence of memory model;
- propose some assistance when verifying the adequation between code and specification of Capla code, e.g., a verified computation of weakest preconditions.

Progress on both objectives will be evaluated through the development of a library of verified Capla functions. An inspiration for such a library could be the WhyMP library for arbitrary-precision integer computations, except that the trusted

computing base would be much smaller and the functions would actually be usable inside formal proofs as if they were pure Coq functions. Of particular interest is Toom-Cook-style multiplication algorithms, as they would exercise some prominent features of the Capla language, e.g., separation of mutable accesses.

If time permits, some other potential research topics are as follows:

- modify the typing and semantics of the Capla language so as to support non-lexical borrows, while preserving both the full verification of the compiler and the ability to prove user programs;
- couple the compiler and the program verification process more tightly, so that some dynamic checks (e.g., in-bounds array accesses) can be optimized away by discharging some proof obligations;
- improve the Capla language and the compiler so as to support richer separation properties, e.g., the lower and upper triangular parts of a matrix are intricately interleaved in memory yet they do not alias.

Skills

A PhD in computer science is mandatory. Knowledge about the semantics of programming languages and their implementation is required. Knowledge of the Coq proof assistant or of a closely-related formal system (e.g., Lean), is highly recommended. Knowledge of French is not required.

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 (90 days / year) 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
- Complementary health insurance under conditions

Remuneration

2788€ gross salary / month

General Information

- **Theme/Domain :** Proofs and Verification
- **Town/city :** Lyon
- **Inria Center :** Centre Inria de Lyon
- **Starting date :** 2025-06-01
- **Duration of contract :** 1 year, 5 months
- **Deadline to apply :** 2025-04-27

Contacts

- **Inria Team :** PASCALINE
- **Recruiter :**
  Melquiond Guillaume / Guillaume.Melquiond@inria.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.

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

Applications must be submitted online on the Inria website.

Processing of applications sent by other channels is not guaranteed.

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.