2018-00396 - [Campagne post-doctorat 2018/CRI PARIS] - Post-doctoral research on modularity, program proof, or memory models

Contract type: Public service fixed-term contract
Level of qualifications required: PhD or equivalent
Fonction: Post-Doctoral Research Visit
Level of experience: Recently graduated

About the research centre or Inria department

Inria, the French National Institute for computer science and applied mathematics, promotes “scientific excellence for technology transfer and society”. Graduates from the world’s top universities, Inria’s 2,700 employees rise to the challenges of digital sciences. With its open, agile model, Inria is able to explore original approaches with its partners in industry and academia and provide an efficient response to the multidisciplinary and application challenges of the digital transformation. Inria is the source of many innovations that add value and create jobs.

Context

The post-doctoral position is located at the Paris research center of Inria, within the Gallium research team (http://gallium.inria.fr/). At Gallium, we conduct research on the design, formalization, and implementation of programming languages and systems. The OCaml language and the CompCert verified compiler embody many of our research results. Our objective is to improve the reliability of software systems through:

- higher-level, safer, more expressive programming languages based on the functional programming paradigm;
- automatic error detection via type systems and related static analyses;
- better linguistic support for formal methods, especially machine-checked proofs of programs.

Assignment

We welcome postdoctoral researchers on topics related to the following three ongoing projects:

1- Verified OCaml library

We are involved in the Vocal project, which aims to build a verified library of basic data structures and algorithms for OCaml. This project offers a wealth of opportunities for challenging proofs of real-world program modules. In these proofs, we often have to deal with mutable state and/or higher-order functions. At least for some modules, we plan to verify the time and/or space consumption of our algorithms. Furthermore, we are facing several fundamental research issues, such as interoperability between the verification tools used in the project, namely Coq, Why3, and CFML: how can we share specifications between these tools, while maintaining consistency? A postdoctoral researcher could contribute to this project by carrying out proofs and/or by improving the metatheory and implementation of our tools.

2- Types, modularity, and program transformations

Our programming languages should encourage modularity, or “programming in the large”. That is, they should make it easy to write small re-usable components and to combine these components while ensuring static type safety and keeping verbosity under control. Unfortunately, many real-world programming languages fail to achieve these properties. Java is very weak. The module systems of Standard ML and OCaml are quite heavyweight, remain surprisingly difficult to formalize, and do not offer an economy of concepts: in OCaml, records, objects and modules are three distinct concepts. We would like to investigate calculi and programming languages that are theoretically more economical, practically easier to use, and more scalable. Rossberg's 1ML and Amin and Rompf's DOT could serve as sources of inspiration. We are interested not only in the theoretical foundations of these calculi, but also in...
language design and usability issues, including type inference. In the presence of universal / existential / dependent types (and other advanced type-theoretic features), it is a challenge to develop (partial) type inference algorithms whose behavior seems predictable to a programmer and is robust in the face of local program transformations. Finally, we are interested in type-directed program synthesis and program transformation, including program evolution and refactoring.

3- Formalization of weak memory models, mixed size extension

Recent work on weak (relaxed) memory models as implemented by contemporary multicore processors addresses "mixed size accesses". "Mixed" size" improves over the simple view of processors atomically accessing independent memory locations: memory accesses are decomposed into several sub-accesses (typically byte accesses) and accesses may be unaligned or overlap. Recent work [1] addresses the issue in the context of operational memory model, where a transition system acts as a model of actual hardware or execution engine.

The DIY suite (http://diy.inria.fr/) provides a formal language (CAT) to describe and implement weak memory models, and tools to verify conformance between these models and actual hardware. By contrast with [1], the models are given in axiomatic style, that is, as conditions that executions has to fulfill to be valid. We are looking forward to extending the modeling machinery and tools so as to handle mixed size accesses. A first objective is to design (and test) a model of "mixed size" x86 machine, with possible extensions to more complex machines and languages (such as C11).


Main activities

Conduct research on one of the topics of interest above.

Skills

Prior research experience is required on:

- For topic 1: mechanized proof, program logics, formal semantics.
- For topic 2: type systems, language design, formal semantics.
- For topic 3: shared-memory concurrency, processor architectures.

Benefits package

- Subsidised catering service
- Partially-reimbursed public transport

Remuneration

- Location: Paris 12ème
- Gross Salary per month: 2 653€ brut/mensuel

Security and defense procedure:

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.