2018-00965 - Towards a system for proving the correctness of concurrent Multicore OCaml programs

Renewable contract : Oui
Level of qualifications required: Graduate degree or equivalent
Fonction : PhD Position

Assignment

This job offer is for a 3-year Ph.D. position in the Gallium team at Inria Paris. The student will be advised by François Pottier (Inria Paris) and Jacques-Henri Jourdan (LRI, Université Paris-Saclay, CNRS).

In short, the main objective of this thesis proposal is to propose, study and implement a system for verifying the correctness of concurrent Multicore OCaml programs (or program modules).

Main activities

Here are a few tasks that we envision should be attacked during (say) the first year of the thesis. This list is not meant to be exhaustive; new research directions should emerge as the work progresses.

1. Based on Dolan et al’s preliminary work, define an operational semantics for (a representative subset of) Multicore OCaml. Mechanise this definition in Coq. Confront it with the experts’ understanding of the language and its memory model.
2. (Optional) Based on this operational semantics, prove that Multicore OCaml is type-safe, that is, well-typed programs do not crash.
3. Following Kaiser et al’s approach, define on top of Iris a program logic for Multicore OCaml. Prove that it is sound, that is, if the rules of the logic allow deducing that a program is correct, then this program is actually correct. Implement this program logic inside Coq.
4. As a benchmark for the expressiveness and usability of the program logic, identify a few key concurrent data structures that should be shipped with Multicore OCaml. (The list of potential candidates is long: hash tables, stacks, queues, bags, work-stealing queues, locks of various kinds, channels of various kinds, barriers, nonzero indicators, exchangers, snapshot algorithms, consensus objects, etc.) Implement some of them. Identify which of them can be proved in the program logic (if so, do it) and which cannot (if so, why? and can the logic be extended?). Also, look for examples of high-level concurrent data structures (which are implemented in terms of one or more lower-level data structures).
5. In parallel with all of the above, look for prototypical applications of Multicore OCaml, that is, applications of OCaml where the use of shared-memory concurrency is both challenging and expected (or hoped) to yield significant performance improvements as the number of cores grows. Implement one (or more) such applications as a way of testing and demonstrating the usability of Multicore OCaml and as a source of inspiration for challenges in program verification.

Benefits package

- Subsidised catering service
- Partially-reimbursed public transport

General Information

- Theme/Domain : Proofs and Verification, Software engineering (BAP E)
- Town/city : Paris
- Inria Center : CRI de Paris
- Starting date : 2018-10-01
- Duration of contract : 3 years
- Deadline to apply : 2018-08-20

Contacts

- Inria Team : Gallium
- Recruiter : Pottier Francois / francois.pottier@inria.fr

About Inria

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 2700 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.

Conditions for application

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.

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.