2019-01991 - Post-Doctoral Research Visit F/M Interactive Verification of Synchronous Programming Languages

Type de contrat : CDD
Contrat renouvelable : Oui
Niveau de diplôme exigé : Thèse ou équivalent
Fonction : Post-Doctorant
Niveau d'expérience souhaité : Jusqu'à 3 ans

Contexte et atouts du poste

Le FidElR project, for "Fidelity in Reactive Systems Design and Compilation", is funded by a French government “Young Researcher” grant (ANR JCJC). Its goal is to extend the Vélus verified Lustre compiler to support more general, actor-based state machines and techniques for interactively verifying models. The grant includes funding for national and international travel to participate in workshops and conferences.

Lustre is a synchronous language closely related to the industrial Scade tool which supports Model-Based Development (MBD) of critical embedded control software. It’s a programming language with a formal semantics for block-diagram specifications.

The Vélus compiler is developed in OCaml and the Coq Interactive Theorem Prover (ITP). It successively transforms source programs into the Clight language used by CompCert. The overall correctness theorem states that the stream-based semantics of the source program is preserved by the generated assembly code.

Vélus is developed in the Inria PARKAS team located at the École normale supérieure in the heart of Paris. Development is led by [Timothy Bourke](https://www.tbrk.org) and involves collaboration with experts in synchronous languages (Marc Pouzet), verified compilation (Xavier Leroy) and automatic verification (Cesare Tinelli).

Mission confiée

Work on Vélus has to date focused on verified compilation. This postdoctoral position would involve developing techniques and tools for interactively verifying Lustre programs within Coq. That is, making it possible to load a Lustre program into Coq, to state invariants, and to prove that the program satisfies them. The compiler correctness theorem guarantees that such invariants also hold of the generated code. While interactive frameworks exist for imperative languages, like the Verified Software Toolchain and Isabelle/FRAMA, and model checkers exist for synchronous languages, like Kind 2 and Lessar, there are relatively few results on the interactive verification of languages for model-based development. We believe that ITPs provide an ideal environment for decomposing verification goals, safely mixing results from model-checkers and specialized tactics, and transferring properties of the model to generated executables.

The postdoctoral researcher will collaborate closely with other team members to develop techniques and tools for interactively verifying Lustre programs in the context of the Vélus project. Please see the Vélus website for scientific references. This work will involve mastering the existing semantic models, proposing verification techniques, implementing plugins and tactics in the Coq ITP and working on case-studies to guide and evaluate the approach. Results will be communicated to international workshops, conferences, and journals.

The initial contract is for one year, but solid progress on research goals would open other opportunities.

Principales activités

1. Master relevant background knowledge on synchronous languages and the state-of-the-art in interactive program verification by reading books and research articles.
2. Experiment with small examples in the Coq ITP to understand the problem and potential solutions.
3. Propose verification techniques and implement them as Coq plugins and tactics.
4. Evaluate the techniques and implementations on one or more larger case studies.
5. Document the results in technical reports and scientific articles.

Additional activities:

1. Participate in workshops and team activities.
2. (Optional) Teach at the L3 and masters level.

Compétences

Technical skills and level required:

- Strong expertise in one or more programming languages (ideally a strongly typed functional language like OCaml, SML, or Haskell).
- Some experience with interactive theorem proving or a very strong motivation to become a specialist.

Languages: French or English.

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 (ick 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.