Offer #2024-08472

Verification of Clock Discipline Algorithm in Coq

Level of qualifications required : Graduate degree or equivalent

Fonction : Internship Research

About the research centre or Inria department

The Inria center at the University of Rennes is one of eight Inria centers and has more than thirty research teams. The Inria center is a major and recognized player in the field of digital sciences. It is at the heart of a rich ecosystem of R&D and innovation, including highly innovative SMEs, large industrial groups, competitiveness clusters, research and higher education institutions, centers of excellence, and technological research institutes.

Assignment

Context:

“Real-time model checking is really simple.” As advertised by Leslie Lamport in [3], the real passage of time can be encapsulated explicitely in TLA+ using a *now* variable that increments with a*Tick* action. As a consequence, the model checking of real-time properties is easier, without necessarily requiring all the complex background details.

Yet, a model differs from the code that executes on a machine, unless proven otherwise. This is the main result of CompCert [2], a verified compiler for the C language, that certifies that the semantics of an executable coincides with the semantics of the source code. However, the semantic preservation theorem does not yet include real time guarrantees.

As CompCert explicitly says in its documentation, the semantic preservation theorem ensures that observable behaviours of the source and target programs are the same, and define observable behaviour as “everything the user of the program, or the physical world in which it executes, can *see* about the actions of the program, with the notable exception of execution time and memory consumption.”.

Challenge:

In this work, we will focus on a specific time sensitive algorithm: the Clock Discipline Algorithm [6]. The algorithm synchronizes a high frequency clock that may accumulate drifting, with a low frequency clock that is reliable. Typically, this algorithm is employed to secure local time on an operating system from the source time given by an external reliable source (i.e., via NTP).

The Clock Discipline algorithm estimates the difference between the two clocks, so that a reading of the local clock can be reliably converted as a value on the source reliable clock.

We will implement this algorithm in software (in a fragment of C), and use a certified compiler to generate code. Moreover, we will prove that the bound estimations given by the algorithm, under assumption verified by the hardware, are realistic and preserved through compilation. The challenge will therefore be to port some of the existing proving technics for memory-safe programs [1], to deal with time-dependent registers (such as [5]).

Practical details:

- supervised by Benjamin Lion;
- funded by the cert-t project;
- gratification;
- integration in the Epicure team at Inria Rennes.

Collaboration :

The recruited person will be in connection with the Epicure team at the Inria center of the university of Rennes.

Main activities

Mission:

The verification of the clock discipline algorithm decomposes into three main goals:

1. Identification of a suitable formalism to formalize the Clock discipline algorithm in Coq.
   The clock discipline algorithm has time-dependent instruction. We will use a simple time model, similar to the time-stamp counter register in modern processor, to reason about correctness of the algorithm. For instance, in [6], it says that "It is possible to convert the discretized time reports of the clocks to continuous time readings by assuming that the associated counter increments once in one period, and by ignoring residual time error within one period."

2. Implementation of the model in a low level language, such as Clight.
   This step requires to get familiar with the Clight syntax and its semantics. Several extensions will need to be considered, to express time syntactically and semantically, such as in [4].

3. Practical generation of certified code on a specific plateform.
   The third objective is to setup a toolchain to generate executable and testable code on some specific architecture. Then, the performance of the generated code could be evaluated with respect to the model prediction.

The set of goals is ambitious, which implies that some of the goals might not be fully completed given the duration of the internship.

Skills

Skills:

- Familiarity with formal semantics, eg. proof assistant, type theory.
- Solid understanding of mathematics, especially algebra.
- Experience with category theory is a plus.
- Analytical and modeling skills: writing specifications, requirement documents, and user documentation

Benefits package

- Subsidized meals
- Social, cultural and sports events and activities

General Information

- **Town/city :** Rennes
- **Inria Center :** Centre Inria de l'Université de Rennes
- **Starting date :** 2025-02-01
- **Duration of contract :** 6 months
- **Deadline to apply :** 2025-02-01

Contacts

- **Inria Team :** AT-REN AE
- **Recruiter :**
  Lion Benjamin / benjamin.lion@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

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.