Offre n°2024-08472

Verification of Clock Discipline Algorithm in Coq

Le descriptif de l'offre ci-dessous est en Anglais

Niveau de diplôme exigé : Bac + 5 ou équivalent

Fonction : Stagiaire de la recherche

A propos du centre ou de la direction fonctionnelle

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.

Mission confiée

Context:

"Real-time model checking is really simple." As advertised by Leslie Lamport in [3], the real passage of time can be encapsulated explicitly 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.

Principales activités

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.

Compétences

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

Avantages

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

Informations générales

- **Ville :** Rennes
- **Centre Inria :** Centre Inria de l'Université de Rennes
- **Date de prise de fonction souhaitée :** 2025-02-01
- **Durée de contrat :** 6 mois
- **Date limite pour postuler :** 2024-12-31

Contacts

- **Équipe Inria :** AT-REN AE
- **Recruteur :**
  Lion Benjamin / benjamin.lion@inria.fr

A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines. L'institut fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. 900 personnels d'appui à la recherche et à l'innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 200 start-up. L'institut s'efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

> **Attention** : Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.

Consignes pour postuler

Sécurité défense :
Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini dans l'arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l'annulation du recrutement.

Politique de recrutement :
Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation

de handicap.