Offre n°2025-08545

PhD Position F/M Resource-Aware Conservative Static Analysis

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

Type de contrat : CDD

Niveau de diplôme exigé : Bac + 5 ou équivalent

Fonction : Doctorant

A propos du centre ou de la direction fonctionnelle

The Inria University of Lille centre, created in 2008, employs 360 people including 305 scientists in 15 research teams. Recognised for its strong involvement in the socio-economic development of the Hauts-De-France region, the Inria University of Lille centre pursues a close relationship with large companies and SMEs. By promoting synergies between researchers and industrialists, Inria participates in the transfer of skills and expertise in digital technologies and provides access to the best European and international research for the benefit of innovation and companies, particularly in the region.For more than 10 years, the Inria University of Lille centre has been located at the heart of Lille's university and scientific ecosystem, as well as at the heart of Frenchtech, with a technology showroom based on Avenue de Bretagne in Lille, on the EuraTechnologies site of economic excellence dedicated to information and communication technologies (ICT).

Contexte et atouts du poste

The PhD student will be part of theSyCoMoRES team of Inria Lille & CRIStAL lab, which currently hosts 4 fellow PhD students and one postdoc. Lille is a city close to Brussels, Paris & London, easily reachable by train, with a large student population and a number of cultural places & events. The lab has a very active equality and parity commission, which raises awareness on this topic to all staff (with specific events for newcomers), and provides outreach activities for high-schoolers. One of the advisors (Raphaël Monat) is an active member of this commission.

PhD students are appointed for a duration of 3 years. We plan to organize weekly research meetings with the PhD student. In addition, the student will be able to attend monthly meetings with other Mopsa practitioners. This research project is part of ANR JCJC RAISIN. We will hold quarterly project meetings with Sophie Cerf (member of the project), who is a researcher at Inria with expertise in control theory for software systems

Mission confiée

Start date flexible. Informal enquiries are welcome by email, reach out toRaphaël Monat

One approach aiming at reducing the number of bugs is static program analysis through the framework of abstract interpretation [1]. Contrary to dynamic analyses such as fuzzing [7], the program is not executed but its source code is analyzed. Thanks to this approach, the analysis conservatively considers all possible execution paths of the program during the analysis, ensuring the absence of false negatives. In addition, the analyses are automatic: they do not require any user interaction to complete their task and they will be completed in a guaranteed finite time. These analyses can be seen as "push-button" as no expert knowledge is required to run them. This approach has been particularly successful to certify the absence of runtime errors in critical embedded C software. Astrée [2] has proved the absence of runtime errors in software of Airbus planes.

The daily use of conservative static analyzers by non-experts remains a challenge. First, these tools offer a wide range of configuration options which is difficult to choose from. Each option will have a different impact on the performance-precision tradeoff of the analysis, that will also vary depending on the considered program. Mansur et al. [5], Heo et al. [3] have looked into ways to automatically choose options to attain the highest precision when analyzing a program, given a resource envelope (CPU time, memory usage); but their approaches are however limited in terms of scalability. Second, most static analyzers cannot express their progress during an analysis, which results in an unfriendly black-box behavior. The overall goal of this thesis is to address these two usability barriers. We plan to explore the following research directions:

- Estimating the experimental complexity of analyzing a given program. In the static program analyses

we consider, we hypothesize that the complexity of analyzing a program is mostly impacted by the number of programs loops and function calls, the maximum depth of these nested constructs. We will need to confirm this hypothesis, and then focus on finding measures of the complexity of a program's analysis. We will start by considering a simplified setting focusing on a toy imperative language. In a way, this complexity measure will be an analysis of the program analysis itself. If needed, we will consider additional, yet realistic, hypotheses on the convergence of widening used during loop analysis.
· Estimation of remaining analysis time. This estimation will be performed online (i.e, during the analysis), when the full configuration of the static analyzer is fixed. Current static analyzers are often guaranteed to terminate in finite time, but do not provide any estimate of the remaining analysis time. We plan to go beyond the work of Lee et al. [4] by developing a semantic, language-independent and domain-independent progress bar that will work with fully relational numerical abstract domains.
· Offline choice of best configuration. We plan to develop techniques finding the configurations yielding the most precise analyses of a given program. We will start by investigating a posteriori techniques where the analyzer suggests precision improvements to remove some of the alarms it found (e.g, by suggesting to enable specific options). We will then consider a priori techniques relying on pre-analyses to find the best configuration options to analyze a program. Combined with an estimation of the cost of analyzing the program in a given configuration, we will be able to find a configuration reaching the best precision while respecting a pre-specified resource envelope. We will leverage the partial order on the precision of analyzers to guide our exploration.

Principales activités

The candidate will work in the overall field of formal methods and programming language theory. They will work on conservative static analyses, and in particular some rooted in the framework of abstract interpretation. We expect the successful candidate to be motivated to improve experimental research tools such as Mopsa, which is implemented in the OCaml functional programming language.

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 (sick children, moving home, etc.)
- Possibility of teleworking 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
- Social security coverage

Informations générales

- **Thème/Domaine :** Preuves et vérification
- **Ville :** Villeneuve d'Ascq
- **Centre Inria :** Centre Inria de l'Université de Lille
- **Date de prise de fonction souhaitée :** 2025-09-01
- **Durée de contrat :** 3 ans
- **Date limite pour postuler :** 2025-04-14

Contacts

- **Équipe Inria :** SYCOMORES
- **Directeur de thèse :**
  Monat Raphael / raphael.monat@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.