Amélioration d'un Analyseur Statique pour les programmes manipulant des tableaux

Mots clés : Analyse statique, Interprétation Abstraite, Preuve automatique, Méthodes Formelles, Tableaux, Sûreté, Cyber-sécurité

Cadre du stage

Le CEA LIST est un centre de recherche technologique sur les systèmes à logiciel prépondérant qui mène ses recherches en partenariat avec les grands acteurs industriels (nucléaire, automobile, aéronautique, défense et médical) pour étudier et développer des solutions innovantes adaptées à leurs besoins. Au sein du CEA LIST, le Laboratoire Sûreté des Logiciels (LSL), localisé à Palaiseau (Essonne), développe les outils d'aide à la validation et à la vérification de logiciels et de systèmes matériels / logiciels tout particulièrement dans les domaines des systèmes embarqués critiques et de la cybersécurité.

L'un des nos outils, nommé Frama-C (http://frama-c.com), est une plate-forme logicielle *open-source* développée en OCaml, facilitant le développement d'analyses de programmes C. Le stage se déroulera au sein de l'équipe développant Frama-C.

Objectifs du stage

L'interprétation abstraite est une technique d'analyse statique permettant de calculer automatiquement les différents comportements du programme et ses propriétés. Cela permet notamment de prouver l'absence de bugs. On utilise pour cela des *abstractions* pour représenter les objets manipulés par les programmes : entiers, flottants, chaines de caractères, structures et tableaux... Par exemple, l'ensemble des valeurs possible pour une variable entière peut être abstrait par un intervalle.

Le but du stage est de développer de nouvelles abstractions pour les tableaux dans les outils d'interprétation abstraite du laboratoire. Ces nouvelles abstractions permettront d'explorer des nouveaux compromis entre précision et temps d'analyse.

Le stage consistera à implémenter différentes étapes de difficulté croissante. (Le nombre d'étapes à réaliser dépendra de la durée du stage, des difficultés rencontrées ou des nouvelles perspectives identifiées durant le stage)

1. Implémenter la technique de " Array smashing " consistant à approximer le tableau d'un seul bloc.
2. Ajouter un partitionnement du tableau par *tranches* correspondant à des intervalles d'indices dont les bornes sont constantes.
3. Perfectionner le partitionnement pour prendre en compte des bornes d'intervalle *symboliques*.
4. Accroitre la précision du partitionnement en exploitant des relations numériques entre les indices.
5. Étendre le modèle précédent en permettant aux tranches de se chevaucher et le rendre ainsi adéquat aux algorithmes les plus complexes.
6. Recherche de propriétés relationnelles entre parties de tableaux

L'implémentation pourra être validée sur des extraits de code industriel critique.

Le stage permettra à l'étudiant de découvrir des méthodes formelles et de de contribuer au développement d'un logiciel *open-source*.

Candidatures

- **Profil**
  - Étudiant niveau M1 ou M2 ou en seconde ou troisième année d'école d'ingénieur
  - Connaissance d'au moins un langage impératif, de préférence le langage C
  - Appétence pour les mathématiques mais aucun prérequis n'est nécessaire
  - La connaissance du langage OCaml est un plus
  - Capacité de travail en équipe
- **Durée** : 2 à 6 mois, les objectifs peuvent être adaptés selon la durée du stage.
- **Conditions** : stage indemnisé, aide au logement possible, transports CEA en Île-de-France.
- **Encadrement** : Valentin Perrelle (*valentin.perrelle@cea.fr*), Matthieu Lemerre (*matthieu.lemerre@cea.fr*)

Les délais administratifs de recrutement au CEA étant de 2 à 3 mois minimum, merci de prendre contact le plus tôt possible.