

Reverse engineering: Software contract inference

Grégoire MENGUY
CEA LIST
gregoire.menguy@cea.fr

Les contrats de fonctions, sous la forme de pré- / post-conditions, permettent de spécifier le comportement de fonctions. Ces contrats sont donc cruciaux pour améliorer la sécurité des programmes et réaliser différentes tâches, de l'ingénierie logicielle à la vérification de code. Malheureusement, ceux-ci sont rarement fournis et doivent donc être rétro-ingéniés à la main.

Récemment, l'algorithme PreCA a été proposé pour inférer, via du machine learning symbolique, des contrats de fonctions automatiquement et avec des garanties fortes de correction. Bien que très prometteuse, cette approche n'en est qu'à ses balbutiements et n'a été appliqué que sur des problèmes simples. Ce projet propose donc d'appliquer PreCA à des programmes plus complexes comme des bibliothèques cryptographiques ou du logiciel embarqué. L'objectif sera ainsi d'exhiber les défis scientifiques et techniques liés à l'utilisation de PreCA et de proposer des extensions pour les dépasser, ainsi que de comparer en profondeur PreCA aux approches de synthèse de spécification développées dans la communauté des méthodes formelles.

Le projet se déroulera comme suit:

- Comprendre le framework d'inférence de précondition PRECA;
- L'évaluer sur un jeu de données de codes réels plus complexes pour étudier ses forces et ses limitations actuelles, par rapport à l'état de l'art;
- Proposer une extension pour pallier à ces limitations et l'implémenter dans PRECA;
- Évaluer cette extension pour prouver son efficacité en pratique.

1 Livrables attendus

Les principaux livrables attendus sont:

- Un résumé des recherches bibliographiques menées;
- Une implémentation documentée de l'extension proposée;
- Le rapport final incluant les deux premiers livrables et le récapitulatif des démarches suivies et des résultats obtenus.

2 Éléments logistiques

Des points réguliers seront organisés avec l'encadrement. Ils pourront être réalisés en visioconférence ou au CEA sur le site Nano-Innov à Saclay.

3 Postuler

Pour postuler, les étudiants doivent contacter l'encadrant par mail.