Département d'Informatique de l'Ecole Normale Supérieure

Abstraction de Relations entre États de la Mémoire

Lieu du stage : École Normale Supérieure ; 45, rue d'Ulm ; 75 230, PARIS.

Équipe concernée dans le laboratoire : Équipe Sémantique et Interprétation Abstraite / Équipe-Projet "Abstraction".

Encadrement & Contact : Xavier RIVAL (*e-mail* : `rival@di.ens.fr`, tél : 01 44 32 21 50, fax : 01 44 32 21 51)

Contexte du stage :

L'analyse de propriétés de formes [1] (ou "*shape analysis*") vise à découvrir des propriétés sur des structures de données de taille non bornée, généralement allouées dynamiquement telles que des listes ou des arbres. Ces structures utilisent généralement des chaînes des pointeurs. L'analyse de programmes contenant des appels de fonctions peut se faire de plusieurs manières, soit en analysant chaque fonction dans son ou ses contexte(s) d'appel(s), soit en calculant une sur-approximation de la relation entre les entrées et les sorties de chaque fonction [2]. L'inconvénient de cette approche est qu'il est difficile de définir une bonne abstraction pour les relations entre entrées et sorties d'une fonction. Dans ce stage, nous proposons de définir un domaine abstrait, utilisant une représentation déduite de celle utilisée dans [1] afin d'approximer des ensembles de telles relations.

Travail souhaité :

La première étape de ce stage consiste à formaliser un domaine abstrait pour représenter des ensembles de relations entre entrées et sorties de fonctions manipulant des états mémoires contenant des structures de données dynamiques. Dans un second temps, on définira les fonctions de transfert associées à l'analyse de chaque composant d'une fonction ainsi qu'un opérateur d'élargissement ; chacun de ces opérateurs devra être prouvé correct par rapport aux opérations concrètes correspondantes. Enfin, on pourra utiliser ce domaine abstrait pour la réalisation d'une analyse modulaire.

Le stage donnera également lieu à une implémentation, qui pourra se faire à partir de l'analyseur **MemCAD**. Dans cette phase, on pourra étudier dans quels cas une analyse modulaire se révèle plus précise ou plus efficace qu'une analyse monolithique. Des expérimentations pourront être menées à partir de bibliothèques d'algorithmes pour structures de données simples ou bien du micro-noyau Minix.

De plus, dans le cadre de ce projet, un financement de thèse est disponible (ERC **MemCAD**).

Pré-requis :

Pour ce stage, il est préférable que l'étudiant ait suivi le cours "2–6 Interprétation Abstraite : Application à la vérification et à l'analyse statique".

Références

[1] Bor-Yuh Evan Chang et Xavier Rival. Relational inductive shape analysis. In POPL'08, pages 247–260, 2008.

[2] Bertrand Jeannet, Denis Gopan, Thomas W. Reps. A Relational Abstraction for Functions. In SAS'05, pages 186-202, 2005.