Département d'Informatique de l'Ecole Normale Supérieure

Analyse Statique de Programme Manipulant des Structures Complexes avec Partage

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 (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.

Des familles d'analyses comme [1] (définie dans le cadre du projet **Xisa** —eXtensible Inductive Shape Analyzer—, `http://xisa.cs.colorado.edu/`) ont été proposées afin d'exprimer et d'inférer des propriétés inductives sur ces chaînes de pointeurs ; elles permettent ainsi de traiter des structures dynamiques au cours d'analyses statiques par Interprétation Abstraite, et de prouver que de telles structures sont préservées, ou bien plus simplement que les accés à la mémoire ne provoquent pas d'erreurs à l'exécution (comme le déréférencement d'un pointeur nul ou invalide).

Ce type d'analyse reposant sur la logique de séparation a pour avantage de traiter avec précision des structures de données avec peu de partage (comme des variantes de listes ou d'arbres).

Toutefois, les structures de données dans lesquelles de nombreuses cellules sont référencées par un nombre non borné de pointeurs sont beaucoup plus difficile à traiter. C'est le cas de structures telles que les graphes, les arbres avec partage (DAG ou "directed acyclic graphs") ou les "union-find". Pour exprimer que de telles structures sont correctes, il faut raisonner sur des ensembles de pointeurs de taille non bornée, et sans structure régulière (au contraire des listes ou des arbres qui peuvent être définis par récurrence).

Travail souhaité :

Le but de ce stage est de mettre au point un domaine abstrait inspiré de celui de [1], et qui permette de traiter de structures reposant sur le principe de partage de sous structures. On utilisera un sous-domaine abstrait pour exprimer des propriétés d'ensembles de valeurs et on proposera une structure permettant de quantifier sur un tel ensemble, à l'intérieur du domaine abstrait consacré aux propriétés sur la mémoire.

Au cours du stage, on formalisera cette analyse et on prouvera sa correction.

Le stage donnera également lieu à une implémentation, qui pourra se faire dans le cadre de l'analyseur **MemCAD**. 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" ou le cours "C–1–10 Fondements de l'Interprétation Abstraite".

Références

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