Sujet de stage L3 ENS
année 2013 - 2014

Didier Galmiche - Daniel Méry
Equipe TYPES, LORIA UMR 7503

Titre : Preuves en logique de séparation quantitative

Thématique.

La logique de séparation de O'Hearn et Reynolds (SL) [7, 8] est un formalisme permettant de raisonner sur des programmes qui transforment des structures de données récursives (listes, arbres, ...) au cours de leur exécution. SL est un modèle concret d'une variante booléenne de la logique de ressources BI dans lequel les ressources sont des cellules de mémoire, arrangées sous forme de tas, que des opérateurs spécifiques ($\wedge$, $*$ et $-\!\!*$) permettent de partager, séparer et mettre à jour. L'un des intérêts majeurs de la logique de séparation est sa propension au *raisonnement local* : les seules ressources qui nécessitent d'être prises en compte dans l'analyse d'un programme sont celles que le programme manipule effectivement. Le raisonnement local permet donc d'entrevoir (à long terme) la définition de méthodes d'analyse plus modulaires.
A l'heure actuelle, l'essentiel des travaux sur l'analyse de programme dans le contexte de la logique séparation sont fondés sur un fragment appelé $\Pi\Sigma$ [2], qui est une extension du noyau propositionnel de SL introduisant des prédicats récursifs de la forme $ls(a, b)$ pour représenter des listes simplement chaînées s'étendant entre deux emplacements mémoire (adresses) a et b [1].

D'une manière générale, la logique de séparation est indécidable, même sans prédicats récursifs [5], même réduite à des tas mémoire avec un seul sélecteur [4]. D'autres travaux ont proposé une extension quantitative de la logique de séparation appelée SQL[3], incluant des contraintes arithmétiques sur la longueur des listes par l'intermédiaire de prédicats de la forme $ls^k(a, b)$, où k est la longueur de la liste s'étendant entre les adresses a et b. Une telle extension est utile pour spécifier des propriétés de correction ou de terminaison, hélas elle est indécidable en toute généralité. Leur seul fragment décidable connu à ce jour est le fragment purement existentiel.

Sujet.

Parmi la grande variété d'approches et de techniques déployées pour l'analyse de spécifications en logique de séparation (model-checking, automates à compteurs, interprétation abstraite, ...), l'approche par recherche de preuves apparaît presque inexistante.
En partant du système de tableaux pour le fragment propositionnel de SL [6], le but du sujet est d'étudier et de proposer des extensions permettant de traiter le cas de la logique de séparation quantitative QSL réduite au cas des listes simplement chaînées de longueur fixée.

Les différentes étapes de ce travail sont :

- l'étude des systèmes de preuves et de construction de contre-modèles proposés pour SL et la logique BI dont elle est un modèle concret ;
- la proposition de méthodes de preuves à base de tableaux pour la logique de séparation quantitative SQL, réduite au cas des prédicats représentant des listes simplement chaînées d'une longueur fixée ;

Renseignements. Le stage aura lieu au sein de l'équipe TYPES du LORIA à Nancy. Pour tout renseignement complémentaire sur ce sujet, contacter D. Galmiche et D. Méry (e-mail : galmiche@loria.fr, dmery@loria.fr).

Références

[1] J. Berdine, C. Calcagno, and P. O'Hearn. A decidable fragment of separation logic. In *FST&TCS'04*, volume 3328 of *LNCS*, pages 97–109. Springer, 2004.

[2] J. Berdine, B. Cook, D. Distefano, and P. O'Hearn. Automatic termination proof for programs with shape-shifting heaps. In *CAV'06*, volume 4144 of *LNCS*, pages 386–400. Springer, 2006.

[3] M. Bozga, R. Iosif, and S. Perarnau. Quantitative separation logic and programs with lists. In *IJCAR'08*, volume 5195 of *LNCS*, pages 34–49. Springer, 2008.

[4] R. Brochenin, S. Demri, and E. Lozes. On the almighty wand. In *CSL'08*, volume 5213 of *LNCS*, pages 322–337. Springer, 2008.

[5] C. Calcagno, H. Yang, and P. O'Hearn. Computability and complexity results for a spatial assertion language for data structures. In *FST&TCS'01*, volume 2245 of *LNCS*, pages 108–119. Springer, 2001.

[6] D. Galmiche and D. Méry. Tableaux and resource graphs for separation logic. *Journal of Logic and Computation*, 20 :1, pp 189-231, 2010.

[7] S. Ishtiaq and P. O'Hearn. BI as an assertion language for mutable data structures. In *28th ACM Symposium on Principles of Programming Languages, POPL 2001*, pages 14–26, London, UK, 2001.

[8] P. O'Hearn, J. Reynolds, and H. Yang. Local reasoning about programs that alter data structures. In *15th Int. Workshop on Computer Science Logic, CSL 2001, LNCS 2142*, pages 1–19, Paris, France, 2001.