Dérivation symbolique d'interpréteur abstrait en Coq

Keywords Preuve de programme, Interprétation abstraite, Assistant de preuve
Main advisor David Pichardie (`David.Pichardie@irisa.fr`)
Second advisor Thomas Jensen (`Thomas.Jensen@irisa.fr`)
Localisation Équipe Celtique IRISA/Inria, Rennes

L'analyse statique est un outil essentiel pour vérifier la sécurité d'un logiciel ou pour prouver l'absence d'erreurs à l'exécution. L'interprétation abstraite [3] propose un cadre mathématique riche pour prouver la correction des analyses statiques de programme. La correction d'une analyse est prouvée par rapport à sa sémantique formelle. La théorie de l'interprétation abstraite propose un cadre pour prouver la corection à partir d'une fonction d'abstraction α et de concrétisation γ

$$C \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} A,$$

qui lient propriétés concrètes et valeurs abstraites. La propriété de correction s'exprime alors comme

$$P \subseteq \gamma \circ P^\sharp \circ \alpha,$$

stipulant que tous les comportements concrets P d'un programme doivent être sur-approximés par l'interprétation abstraite $P^\sharp$ du programme. Dans des travaux antérieurs, nous avons montré comment utiliser ce cadre théorique pour prouver des analyseurs statiques dans l'assistant de preuve Coq [2, 4].

Pourtant, jusque là, une partie importante de ce cadre a été ignorée : les fonctions d'abstraction (notées α) qui permettent de spécifier formellement les choix optimaux que l'on peut effectuer lors de la conception d'une analyse, nécessairement approchée. L'utilisation d'un tel outil théorique en Coq ouvre la porte vers la dérivation symbolique d'une implémentation d'une analyse, à partir de sa spécification. Plus précisement, l'analyse optimale d'une fonction est définie par l'expression $\alpha \circ P \circ \gamma$ mais cette expression ne donne pas une définition explicite de l'abstraction optimale. Cependant, des dérivations symboliques permettent parfois obtenir une bonne approximation, qui sera correcte par construction.

L'objectif de ce stage est d'étudier le calcul d'un tel opérateur dans la logique de l'assistant de preuve Coq. Le but est de développer un ensemble de théorèmes et de tactiques permettant de suivre au plus près les techniques de dérivation symbolique récentes [5]. Ces librairies seront mises à l'épreuve sur un langage de programmation simple et des abstractions classiques comme les intervalles. Les travaux réalisés prendront la suite d'un precedent stage [1], en ajoutant en particulier des opérateurs de point fixe, et d'autres constructions pertinentes.

Nous recherchons un(e) stagiaire motivé(e) par la preuve de programme et les structures algébriques. Une certaine aisance avec les manipulations ensemblistes est requise. Il est aussi nécessaire de suivre les cours SEM et SOS du master cette année.

Références

[1] Dominique Barbe. Dérivation symbolique d'interpréteur abstrait en coq. Rapport de stage, `http://perso.eleves.ens-rennes.fr/people/Dominique.Barbe/derivationAI_long.pdf`, 2015.

[2] David Cachera and David Pichardie. A certified denotational abstract interpreter. In *Proc. of International Conference on Interactive Theorem Proving (ITP-10)*, volume 6172 of *Lecture Notes in Computer Science*, pages 9–24. Springer-Verlag, 2010. http://people.irisa.fr/David.Pichardie/papers/itp10.pdf.

[3] Patrick Cousot and Radhia Cousot. Abstract interpretation : A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *4th ACM Symposium on Principles of Programming Languages (POPL 1977)*, pages 238–252, 1977. http://cs.nyu.edu/~pcousot/publications.www/CousotCousot-POPL-77-ACM-p238--252-1977.pdf.

[4] Jacques-Henri Jourdan, Vincent Laporte, Sandrine Blazy, Xavier Leroy, and David Pichardie. A formally-verified C static analyzer. In *42nd symposium Principles of Programming Languages*, pages 247–259. ACM Press, 2015. http://people.irisa.fr/David.Pichardie/papers/popl15.pdf.

[5] Jan Midtgaard and Thomas P. Jensen. A calculational approach to control-flow analysis by abstract interpretation. In *15th International Symposium on Static Analysis, (SAS 2008)*, pages 347–362, 2008. http://janmidtgaard.dk/papers/Midtgaard-Jensen%3aSAS08.pdf.