Sujet de thèse 2016-2017

Vérification d'Ordre Supérieur (VérOS)

Direction: Sylvain Salvati

L'objectif de ce sujet de thèse est de proposer des algorithmes efficaces de vérification des programmes d'ordre supérieur. Pour cela, le sujet abordera le problème de l'évaluation des programmes dans un domaine abstrait de façon progressive. Le sujet se développera en trois étapes :

1. adaptation à l'ordre supérieur des méthodes d'interprétation abstraite aux spécifications de sûreté
2. extension aux spécifications comportementales
3. implémentation des algorithmes obtenus sur une partie du langage OCaml

La première partie du sujet consiste à aborder les problèmes liés à des spécifications simples qui garantissent la bonne exécution du programme (l'absence d'erreur à l'exécution). Les fondements théoriques de ces problèmes de vérification sont bien compris : les modèles dénotationels associés (modèles de Scott) et leur décomposition linéaire (modèles relationnels) sont déjà bien étudiés. Il s'agira d'adapter ici les méthodes de l'interprétation abstraite afin d'accélérer l'évaluation des programmes dans ces domaines abstraits. Pour cela, le travail s'orientera vers les méthodes d'analyse du flot de contrôle et essaiera de les coupler avec l'évaluation des programmes dans les domaines abstraits. Il s'agira également de proposer des méthodes adaptatives tenant compte de la structure du modèle afin d'étendre les techniques d'accélération de convergence (widening et narrowing) qui ont fait le succès de l'interprétation abstraite. On cherchera également à isoler des classes de programmes pour lesquels ces problèmes de vérification appartiennent à des classes de complexité relativement basses (PTIME, NP, ou PSPACE).

La seconde partie du sujet consiste à étendre les méthodes développées dans la première partie à des spécifications comportementales, c'est-à-dire des spécifications qui décrivent des comportements infinitaires des programmes. La difficulté à surmonter est que dans ce cadre, les calculs de points fixes ne sont plus extrémaux, ce qui semble faire obstacle aux méthodes d'accélération de convergence qui passent par des approximations pouvant fortement dégrader la précision des calculs de points fixes non-extrémaux. On se concentrera donc sur l'articulation des méthodes d'analyse du flot de contrôle avec l'évaluation du programme dans le domaine abstrait.

La troisième partie s'effectuera en parallèle avec les deux premières et formera le volet expérimental de la thèse. Il s'agira de tester et de vérifier que les méthodes proposées parviennent à traiter les exemples fournis par la littérature. Il s'agira également de comparer ces nouvelles méthodes avec les méthodes existantes.