Proposition de thèse
Assistance à la certification d'outils de composition de services.

Projet Crocus - Équipe ACADIE
Contact : hurault@enseeiht.fr

Titre : Assistance à la certification d'outils de composition de services.

Les systèmes critiques requièrent la certification de leur correction. Les petits systèmes peuvent être développés from scratch, les gros systèmes aux exigences complexes doivent être construits à partir de briques (services) existantes. La preuve de la correction du système est alors composée de deux problèmes distincts : prouver chaque service et prouver que la composition est correcte vis à vis de propriétés globales (l'absence d'interblocage par exemple). Nous nous intéressons au second problème. Étant donné un large ensemble de services, découvrir quelles compositions (et combien de compositions) résolvent un problème est une tâche complexe. Cependant en utilisant la signature, la sémantique et/ou le comportement des services, plusieurs solutions existent pour résoudre ce problème. La découverte et l'adaptation des compositions de services peuvent être automatisées. Il reste alors à prouver que la composition proposée est correcte. Certifier les outils eux-mêmes est une tâche très difficile. Une autre approche est de certifier chaque solution. En effet l'outil peut fournir des indications sur la manière dont la solution a été obtenue, ces informations serviront ensuite à prouver formellement que cette solution est correcte. Pour illustrer, il est bien plus facile de vérifier que 5 est une solution de $x^5 - 4x^4 - 20x^2 + x = 130$ que de certifier un solveur d'équations.

Dans cette thèse, deux outils seront certifiés en utilisant cette approche. Ces outils sont un outil de courtage de service et un comparateur d'automates. Le premier découvre les compositions de services répondant à une sémantique voulue et le second s'assure que les comportements des services composés sont compatibles. Chaque outil donne, en plus de la solution, une trace des actions qu'il a réalisées pour construire la solution. Cette trace sera utilisée pour générer automatiquement une preuve Coq qui donnera la correction de la solution. L'étudiant devra comprendre le fonctionnement des deux outils pour connaître quelles informations sont nécessaires pour la preuve et il devra ensuite utiliser la trace pour générer une preuve Coq et la valider.

Comme exemple, considérons l'outil de courtage. La sémantique des services, ainsi que la requête de l'utilisateur, sont décrits par des termes sur une algèbre. Résoudre le problème de découverte revient alors à résoudre un problème d'unification équationnelle. Pour prouver que la solution rendue par le trader est correcte, il faut traduire l'algèbre décrivant le domaine d'application des services en ensembles, variables et hypothèses compréhensibles par Coq. Les équations sont des hypothèses et l'égalité de la requête et de la réponse modulo les équations est le but à prouver. Pour faire cette preuve, le trader doit indiquer quelle équation est appliquée sur quel sous-terme et dans quel ordre.

Une fois que les deux outils seront certifiés, l'objectif final est de repérer les schémas communs aux deux certifications et de proposer un cadre général pour cette approche de certification.