Proposition de recherche doctorale

Mécanismes objets et changement de représentation de données pour l'interopérabilité entre prouveurs

Mots clés :

- **Directeur de thèse** : Catherine Dubois
- **Co-encadrant(s)** :
- **Unité de recherche** : Centre d'Étude et de Recherche en Informatique et Communications
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

Développer des preuves dans un assistant à la preuve est une activité coûteuse. Par conséquent il est intéressant de pouvoir réutiliser une preuve venant d'un autre outil de preuve que celui utilisé. Même pour des démonstrateurs (automatiques ou non) proches, fondés sur des formalismes logiques proches, ceci n'est guère possible. Des efforts vont dans ce sens par exemple avec le développement de formats partageables par plusieurs assistants comme OpenTheory [3] ou l'idée de l'interopérabilité telle qu'elle est développée dans le système Dedukti [1] (https://www.rocq.inria.fr/deducteam/Dedukti/), à savoir assembler des preuves traduites dans un formalisme commun, le lambda-pi-calcul modulo. Les preuves sont ensuite vérifiées par le vérificateur de type associé appelé Dedukti. Le sujet de cette thèse se place dans ce dernier cadre. Des travaux en cours concernent la traduction de preuves Coq et HOL vers Dedukti. L'objectif principal de la thèse est d'étendre cette famille de traducteurs en étudiant la traduction vers Dedukti de notions et de mécanismes issus du paradigme objet tels que l'objet, la classe, l'héritage simple ou multiple, la redéfinition, la liaison retardée. Le langage FoCaLize (http://focalize.inria.fr/) est un langage qui permet de développer des applications certifiées, c'est-à-dire prouvées correctes par rapport à leurs spécifications. Ainsi il permet de spécifier, implanter et prouver. Et il met en oeuvre des mécanismes orientés objets pour structurer et réutiliser les spécifications, les programmes et les preuves. Le compilateur FoCaLize produit un exécutable Ocaml et un fichier Coq créé à des fins de vérification. Un des objectifs de la thèse est d'appliquer les schémas de traduction généraux des mécanismes objets vers Dedukti afin d'obtenir un compilateur de FoCaLize vers Dedukti, utilisable aux mêmes fins que le compilateur vers Coq. Une première étude de cette compilation a été réalisée pour un sous-ensemble de FoCaLize [2]. Il s'agira donc de l'étendre à tout le langage. Outre ses aspects orientés objets, le langage FoCaLize est un langage fonctionnel (avec des types inductifs et des constructions de filtrage) dont la syntaxe est proche de celle de Ocaml et s'appuie sur le langage des prédicats pour écrire les propriétés. Il est donc en ce sens proche de Coq, il est donc intéressant de se poser la problématique de la réutilisation de preuves Coq au sein de l'environnement FoCaLize. Néanmoins il est fort probable de devoir ajuster les preuves pour qu'elles puissent s'assembler. Par exemple Coq aura défini ses entiers naturels à la Peano alors que FoCaLize les aura définis à l'aide d'une représentation binaire. Nous proposons de munir FoCaLize d'un mécanisme de changement de représentation de données [4], une forme de raffinement de données, qui rendra plus facile l'interopérabilité de FoCaLize et Coq. Références [1] M. Boespflug, Q. Carbonneaux, and O. Hermant. The lambda-pi-calculus modulo as a universal proof language. In International Workshop on Proof Exchange for Theorem Proving, volume 878 of CEUR Workshop Proceedings, pages 28–43, Manchester, UK, June 2012. [2] R. Cauderlier. Object-Oriented Features in lambda-Pi-calculus modulo, Compiling FoCaLize to Dedukti. Master mpri, ENS Cachan, 2012. [3] Joe Hurd. The OpenTheory standard theory library. In NASA Formal Methods, NFM'11, volume 6617 of LNCS, pages 177–191. Springer, 2011. [4] N. Magaud. Changing Data Representation within the Coq System. In TPHOLs'2003, volume 2758. LNCS, Springer-Verlag, 2003.

Résumé du projet de recherche (Langue 2)

Les enjeux scientifiques à relever dans cette thèse sont les suivants : - Extension du compilateur FoCalize vers Dedukti. - Développement de techniques de changement de représentation de données dans le cadre de la déduction modulo et de Dedukti. - Proposition de méthodes de réutilisation de preuves utilisant les techniques de changement de représentation de données précédentes.

Informations complémentaires (Langue 2)

La thèse se fera en collaboration avec l'équipe Deducteam de l'INRIA Rocquencourt, qui développe Dedulti. Elle se fera également en étroite collaboration avec l'équipe de développpement de l'atelier FoCalize.