

Coq-HOL

sujet de stage de M2 2008-2009

Encadrant principal : Benjamin Werner

Lieu : Equipe-projet INRIA Typical, LIX, Ecole Polytechnique

Description

On se propose d'étudier la faisabilité, et si possible de réaliser, une interface permettant d'importer en Coq les preuves réalisées en HOL-light.

Les traductions entre systèmes de preuves sont un champ d'application difficile mais pouvant être riche en retombées. On propose ici une nouvelle technique exploitant les caractéristiques de la théorie des types.

HOL-light est une implémentation de la logique d'ordre supérieur de Church. C'est une variante du système de preuve HOL, réalisée par John Harrison. Elle dispose en particulier d'une bibliothèque d'analyse très développée.

Une approche par reflexion

La logique de Coq est une extension de HOL, à condition de se donner quelques axiomes classiques : tiers-exclu, extensionnalité, opérateur de choix. En simplifiant un petit peu, on se propose de :

- Représenter en Coq les lambda-termes simplement typés par un type Coq `term`.
- Définir pour ces termes une traduction `tr` qui, en particulier, associe des propositions Coq aux termes de type `o`. On pourra utiliser la technique proposée dans l'article de 2007 [1].

On va ensuite définir un type `proof` correspondant aux dérivations dans HOL avec une relation `deriv : term → proof → Prop` qui exprime qu'une dérivation est effectivement une preuve correcte d'une proposition HOL.

On va ensuite prouver que si on a `(deriv t P)` alors la proposition Coq `(tr P)` est vraie (en Coq). Donc on saura transformer les preuves HOL en preuves Coq.

Interface

HOL-light propose différents mécanismes d'exportation de preuves. On va donc ensuite implémenter un traducteur de cette syntaxe vers le type `proof`.

Challenges

Ce travail demande de maîtriser plusieurs outils. La recherche portera sans doute sur les questions suivantes :

- Trouver une représentation suffisamment compacte des preuves HOL (cad. du type `proof`) ; sans doute en utilisant des techniques de partage, d'omission d'étapes de réécriture, etc. . .
- Trouver la bonne formulation des axiomes correspondant à HOL.
- Trouver les bonnes représentations en coq des types de données tels qu'axiomatisés en HOL et intégrer cela à la définition de la traduction `tr`.
- Sans doute plusieurs difficultés imprévues.

Références

- [1] F. Garillot and B. Werner. Simple types in type theory : Deep and shallow encodings. In K. Schneider and J. Brandt, editors, *TPHOLs*, volume 4732 of *Lecture Notes in Computer Science*, pages 368–382. Springer, 2007.
- [2] J. Harrison. Hol light. [http ://www.cl.cam.ac.uk/~jrh13/hol-light/](http://www.cl.cam.ac.uk/~jrh13/hol-light/).
- [3] F. Wiedijk. Encoding the hol light logic in coq. [http ://www.cs.ru.nl/~freek/notes/holl2coq.pdf](http://www.cs.ru.nl/~freek/notes/holl2coq.pdf).