HOL4-Beagle, de l'ordre supérieur vers le premier ordre

Thibault Gauthier

January 5, 2014

Deux façon différentes de démontrer des théorèmes

	Prouveur interactif	Prouveur automatique
Prouveurs	HOL4, Coq, ...	Beagle, SPASS, ...
Expressivité	Ordre supérieur.	Premier ordre.
Efficacité	Guidé.	Automatique.
Sûreté	Petit noyau.	Code assez long.

Énoncé du problème

Problème Voilà deux prouveurs internes à HOL4.

- Metis: ordre supérieur
- Cooper: arithmétique

Énoncé du problème

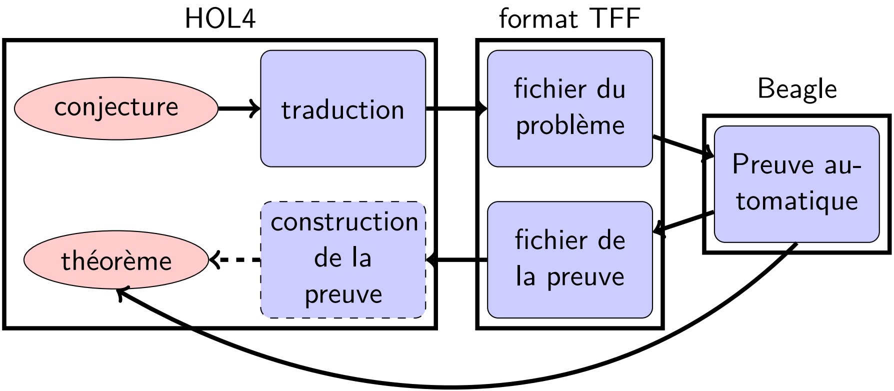
Problème Voilà deux prouveurs internes à HOL4.

- Metis: ordre supérieur
- Cooper: arithmétique

Solution Un prouveur externe.

- Beagle: premier ordre et arithmétique

Schéma d'interaction



Ordre de la traduction vers le premier ordre

1. Monomorphisation
2. Négation de la conclusion
3. Mise en forme normale conjonctive
4. λ-lifting
5. Elimination des booléens
6. Mise sous forme d'un ensemble de clauses
7. Défonctionnalisation
8. Injection des numéraux dans les entiers
9. Instantiation des variables booléennes quantifiées

Monomorphisation

Instanciation des types polymorphes (a,b,...) de HOL4 par des types monomorphes (int,$bool$,...).

Problème

Théorème 1: $\forall y : b.\ D\ y$ Théorème 2: $\forall x : a.\ D\ x \Rightarrow C\ x$
Conjecture : $C\ 2$

Unification du type de $C : a \rightarrow bool$ et de $C : int \rightarrow bool$

Théorème 1: $\forall y : b.\ D\ y$ Théorème 2: $\forall x : num.\ D\ x \Rightarrow C\ x$
Conjecture: $C\ 2$

Unification du type de $D : b \rightarrow bool$ et de $D : num \rightarrow bool$

Théorème 1: $\forall y : num.\ D\ y$
Théorème 2: $\forall x : num.\ D\ x \Rightarrow C\ x$
Conjecture: $C\ 2$

λ-lifting

$$P\ (\lambda x.x + 1)$$

$$\exists f.\ (\forall x.\ f\ x = x + 1) \wedge P\ f$$

Elimination des booléens

$$P(\forall x.\ x = 0)$$

$$((\forall x.\ x = 0) \Rightarrow P\ \mathit{true}) \wedge (\neg(\forall x.\ x = 0) \Rightarrow P\ \mathit{false})$$

Défonctionnalisation

Soit App vérifiant $App\ f\ x = f\ x$. On effectue une défonctionnalisation lorsqu'une fonction non-arithmétique:

- est quantifiée universellement

$$!h.\ h\ x\ y = 0$$

$$!h.\ App\ (App\ h\ x)\ y = 0$$

- a le même type qu'une fonction quantifiée universellement
- a un nombre d'arguments qui varie

$$h\ x\ y\ z \wedge h\ x = g$$

$$App\ (App\ (h\ x)\ y)\ z \wedge h\ x = g$$

.

Qualités et limites de l'interaction HOL4-Beagle

Qualités:

- Résout des problèmes arithmétiques sans guidage
- Utilise un format de communication répandu
- Est correcte et préserve l'insatisfaisabilité

Limites:

- 20% des conjectures prouvées par Metis ne sont pas prouvées par Beagle.
- Est incomplète et ne préserve pas la satisfaisabilité
- Ne génére pas automatiquement des théorèmes aidant à prouver la conjecture
- Ne rejoue pas la preuve