Certification Coq d'un cours de logique de master

Pierre Letouzey

3 septembre 2019

L'informatique, ça peut être assez fumeux...

En cas de doute, suivre le chemin canonique . . .

Pointeurs

- Le cours de “preuves assistées par Ordinateur” (Master1 ici) : https://www.irif.fr/users/letouzey/edu/preuves
- Le poly d'Alexandre Miquel : https://www.irif.fr/~letouzey/preuves/cours.pdf
- Le code Coq (et cet exposé) : https://gitlab.math.univ-paris-diderot.fr/letouzey/natded

Réalisation de cette année

Encodage “profond” d’un calcul des prédicats en Coq

- Déduction naturelle (avec contextes), 1er ordre
- Visée pédagogique (rien de révolutionnaire, mais . . .)
- Basé sur le poly d’Alexandre Miquel
- Modèles classiques (Coq) et théorème de complétude[1]

[1] cas dénombrable

Pourquoi ?

Pas de doute envers ces résultats très standards. Mais:

- Montrer aux étudiants un usage réaliste de Coq
- Venir en appui des preuves méta répétitives *et* délicates
- Illustrer l'aspect mécanisable (un micro prouveur ?)
- Différentes expérimentations (alpha, locally-nameless, . . .)
- A terme : Coq pour corriger les TD de déduction naturelle ?

Littérature

- Des encodages profonds de logique à la pelle
  - Exemple: logique linéaire par O. Laurent
- Cf aussi le POPLMark Challenge pour le codage des lieurs
- Une preuve du théorème de complétude en Isabelle: https://www.isa-afp.org/entries/Completeness-paper.pdf

Lignes de code Coq

```
  201 AsciiOrder.v + StringOrder.v
  526 StringUtils.v + Utils.v
  424 NameProofs.v
  562 Countable.v
  187 Defs.v
  542 Nam.v
  934 Mix.v
  258 Subst.v
 1175 Equiv.v + Equiv2.v
 1842 Meta.v
 1334 Theories.v
  466 PreModels.v
  956 Models.v
  167 Peano.v
  116 FormulaReader.v
 1194 AltSubst.v

10884 total
```

Un aperçu du poly d'origine

Cf https://www.irif.fr/~letouzey/preuves/cours.pdf

En particulier :

- la définition récursive des termes et formules
- la définition de l'alpha-équivalence
- la définition des dérivations de preuves
- les théories de Peano et de ZF
- un example de méta-théorie : le théorème de complétude

Pourquoi ce style de logique ?

- Certes pas de propriété de la sous-formule
- Certes pas propice à l'élimination des coupures
- Mais méta-théorie relativement simple
- Prolongement vers Curry-Howard, ordre supérieur, Coq ...

Points délicats pour les étudiants

- Les variables et l'alpha-équivalence
- Les conditions de bord dans $\forall$-intro et $\exists$-elim
- Lemme de substitution
- Plus généralement preuves méta ennuyantes *et* subtiles

Superficiel / Profond ?

Shallow Embedding / Deep Embedding ?

Comment coder les lieurs ?

- nommé
- indice de De Bruijn
- HOAS
- locally nameless
- ...

Visite guidée des fichiers Coq

Conclusions & Perspectives

A faire:

- Un binaire autonome (micro assistant de preuve)
- Finir quelques bricoles (Théorème de Skolem)
- Théorème d'incomplétude de Gödel ?
- Aspect pédagogique à améliorier (un atelier de preuve ?)
- ZF ?

Plus long terme : d'autres cours Coq-ifiables ?

Photos