

Coq Certification of a Master logic course

Pierre Letouzey

3 September 2019

Off-topic : a pipe-related business in Italy ...



Off-topic : a pipe-related business in Italy ...



Désolé, c'est un peu fumeux...

Off-topic : if lost in Italy, follow the canonical way . . .



Pointers

- ▶ My course “preuves assistées par ordinateur” (Master 1 here) :
<https://www.irif.fr/users/letouzey/edu/preuves>
- ▶ The course pdf by Alexandre Miquel :
<https://www.irif.fr/~letouzey/preuves/cours.pdf>
- ▶ The new Coq development (and this talk) :
<https://gitlab.math.univ-paris-diderot.fr/letouzey/natded>

This year's contribution

Deep encoding of a predicate calculus in Coq

- ▶ Natural Deduction style (with contexts), first order
- ▶ Pedagogical aim (no pioneer work, but not so obvious either)
- ▶ Based as much as possible on Alexandre Miquel's document
- ▶ Classical models (Coq) and completeness theorem¹

¹countable case

Why ?

Pretty unlikely to find bugs in such standard results. But:

- ▶ Shows a realistic usage of Coq to students
- ▶ Helps meta proofs (boring **and** tedious)
- ▶ Highlights the computability (an executable micro prover ?)
- ▶ Different experiments (alpha, locally-nameless, ...)
- ▶ Coq to proof-check students homework on natural deduction ?

Related Works

- ▶ Deep encodings of logics are commonplace
 - ▶ Example: linear logic by O. Laurent
- ▶ See also POPLmark Challenge concerning the binder encoding
- ▶ J. Margetson, 2004 : completeness theorem in Isabelle
<https://www.isa-afp.org/entries/Completeness-paper.pdf>

A glimpse of the reference document

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

In particular :

- ▶ Definition of terms and formulas
- ▶ Definition of alpha-equivalence
- ▶ Definition of proof derivations
- ▶ Concrete theories : Peano, ZF
- ▶ Some meta-theory, for instance the incompleteness theorem

Btw, why this logic ?

- ▶ Ok, no sub-formula property (bad for proof search)
- ▶ Ok, problematic cut elimination
- ▶ But both usage and meta-theory are relatively simple
- ▶ Extension-friendly : Curry-Howard, higher order, Coq ...

Difficult points for students

- ▶ Variables and alpha-equivalence
- ▶ Side-conditions in \forall -intro and \exists -elim
- ▶ Substitution lemma
- ▶ More generally : repetitive **and** subtle meta-proofs

Shallow Embedding / Deep Embedding ?

How to encode binders (quantifiers) ?

- ▶ Named
- ▶ De Bruijn indices
- ▶ HOAS
- ▶ Locally nameless
- ▶ ...

LoC (Lines of Coq)

201 AsciiOrder.v + StringOrder.v

526 StringUtils.v + Utils.v

424 NameProofs.v

187 Defs.v

542 Nam.v

934 Mix.v

258 Subst.v

1175 Equiv.v + Equiv2.v

1842 Meta.v

562 Countable.v

1334 Theories.v

466 PreModels.v

956 Models.v

167 Peano.v

116 FormulaReader.v

1194 AltSubst.v

10884 total

Guided tour of Coq files

Future

To do:

- ▶ A standalone executable program (micro proof-assistant)
- ▶ Skolem theorem (should be obvious now)
- ▶ Gödel incompleteness theorems ?
- ▶ Improve pedagogical aspects (a proof “workshop” ?)
- ▶ ZF ?

More generally, which other courses could benefit from Coq ?