Proof Assistants (MPRI 2-7-2)

Exercise 1

Bruno Barras

January 20th 2017

The goal of this exercise is to show the soundness of a transformation on formulae of first-order predicate logic: the negated-translation.

This translation will be used to derive the consistency of several classical logics w.r.t. their intuitionistic counterparts.

Using an interpretation of formulae as Coq propositions, the consistency of Peano Arithmetic (PA) will be shown.[1]

1 First-order Logic

1.1 Formulae and Derivations

Formulae will be represented by the following inductive type:

```
Inductive form :=
   Tr               (* true *)
 | Fa               (* absurd *)
 | And (_ _:form)   (* conjunction *)
 | Or (_ _:form)    (* disjunction *)
 | Impl (_ _:form)  (* Implication *)
 | All {A:Type} (_:A->form)  (* Universal quantifier *)
 | Ex {A:Type} (_:A->form)   (* Existential quantifier *)
 | Atom (_:Prop).            (* Atomic propositions *)
```

The propositional connectives are encoded straightforwardly. Universal and Existential quantifiers are encoded in a higher-order style. Note the curly braces around the argument A which means that this argument must not be given. Nonetheless, in pattern-matching, `All` and `Ex` will still expect 2 arguments. The last constructor represents atomic propositions, encoded directly within the logic of Coq. For instance,

```
Ex(fun n:nat => Atom(n = 5))
```

[1] Of course, the consistency proof will rely on the assumption that the formalism of Coq is consistent.

represents the formula $\exists n \in \mathbb{N}.n = 5$.

1. Write an inductive family `deriv:(form->Prop)->form->Prop` such that `deriv L f` holds when the sequent $L \vdash f$ holds in *intuitionistic* first-order predicate logic. Each constructor will encode as closely as possible an inference rule of the logic.

Assumptions L (also called theories) are represented as a collection of formulae (expressions of type `form->Prop`), as it allows to represent schematic axioms. For instance, excluded-middle will be the collection of axioms `Or A (Impl A Fa)` for all formulae A.

1.2 Properties of derivations

1. Prove a weakening lemma

```
Lemma deriv_weakening (L L':form->Prop) f :
  deriv L f ->
  (forall f, L f -> L' f) ->
  deriv L' f.
```

Be careful to perform the necessary generalizations before the induction on the derivation!

2. Similarly, prove the cut (or substitution) lemma

```
Lemma deriv_substitution (L L':form->Prop) f :
  deriv L f ->
  (forall f, L f -> deriv L' f) ->
  deriv L' f.
```

2 Negated-translation

2.1 Definition

The idea of the negated translation is to erase all constructive content of a formula by adding double-negation on disjunctions, existential and atomic formulae.
1. Write a function `nnt : form -> form` that implements the negated translation $A \mapsto A^{\mathbf{N}}$ such that:

$$\begin{aligned}
\top^{\mathbf{N}} &= \top \\
\bot^{\mathbf{N}} &= \bot \\
(A \wedge B)^{\mathbf{N}} &= A^{\mathbf{N}} \wedge B^{\mathbf{N}} \\
(A \vee B)^{\mathbf{N}} &= \neg\neg(A^{\mathbf{N}} \vee B^{\mathbf{N}}) \\
(A \Rightarrow B)^{\mathbf{N}} &= A^{\mathbf{N}} \Rightarrow B^{\mathbf{N}} \\
(\forall_T x.P(x))^{\mathbf{N}} &= \forall_T x.P(x)^{\mathbf{N}} \\
(\exists_T x.P(x))^{\mathbf{N}} &= \neg\neg\exists_T x.P(x)^{\mathbf{N}} \\
A^{\mathbf{N}} &= \neg\neg A \text{ for atomic formula } A
\end{aligned}$$

2.2 Soundness of translation

1. Prove the double-negation elimination for translated formula:

$$L \vdash \neg\neg A^{\mathbf{N}} \;\Rightarrow\; L \vdash A^{\mathbf{N}}$$

by induction on the formula. Be careful to generalize over the assumptions L.
2. Prove the soundness of the translation:

$$L \vdash A \;\Rightarrow\; L^{\mathbf{N}} \vdash A^{\mathbf{N}}$$

where $L^{\mathbf{N}}$ is the collection of assumptions $B^{\mathbf{N}}$ for all $B \in L$. The proof is by induction over the derivation.

3 Classical logic

3.1 Definition of classical derivability

We define a theory C (in Coq, a constant `classic : form -> Prop`) of all instances of the excluded-middle. That is, the collection of formulae $A \vee \neg A$ for all proposition A:

```
Inductive classic : form -> Prop :=
  Cem P : classic (Or P (Impl P Fa)).
```

Note that classical logic is obtained by adding `classic` to the set of assumptions. The judgment of derivability in classical logic $\vdash_C$ is defined as

$$L \vdash_C A ::= L \cup \mathrm{C} \vdash A$$

1. Prove that the negated-translation of any axiom of C is provable in any set L.

3.2 Elimination of excluded-middle

1. Prove the elimination of excluded-middle:

$$L \vdash_C A \;\Rightarrow\; L^{\mathbf{N}} \vdash A^{\mathbf{N}}$$

Hint: use the cut lemma.

4 Equality and Arithmetic

4.1 Definition

1. Define the parametric theory E (of type `Type->form->Prop`) of equality that assumes that equality is an equivalence relation. The equality symbol will be represented by the equality of Coq (=) via the atomic constructor: $x = y$ stands for `Atom(x=y)`.

2. Define the theory A of arithmetic that assumes the following Peano axioms:

$$\neg 0 = S(n) \qquad S(m) = S(n) \Rightarrow m = n \qquad P(0) \Rightarrow (\forall_{\mathbb{N}} n.P(n) \Rightarrow P(S(n))) \Rightarrow \forall_{\mathbb{N}} n.P(n)$$

for all m, n and P. The type interpreting the natural numbers will the type `nat` of Coq.
3. Observe that given the properties of the type `nat` and its operation $+$ and $*$, the definition of addition and multiplication are just instances of the reflexivity: $(0 + n = n) \in \mathrm{E}$, etc.

We define Peano Arithmetic (PA) as the conjunction of theories A, E and C and Heyting Arithmetic (HA), the intuitionistic counterpart of PA, as the conjunction of A and E:

$$L \vdash_{PA} A ::= L \vdash_{\mathrm{AEC}} A \qquad L \vdash_{HA} A ::= L \vdash_{\mathrm{AE}} A$$

4.2 Preservation of provability by translation

1. Prove that for both theories E and A the translation of their assumptions are derivable in the theory:

$$P \in \mathrm{E} \Rightarrow \mathrm{E} \vdash P^{\mathbf{N}} \qquad P \in \mathrm{A} \Rightarrow \mathrm{A} \vdash P^{\mathbf{N}}$$

2. Prove that any derivable judgment of PA gives a derivable judgment in HA by negated transalation:

$$L \vdash_{PA} A \;\Rightarrow\; L^{\mathbf{N}} \vdash_{HA} A^{\mathbf{N}}$$

5 Consistency of Peano Arithmetic

5.1 Interpretation of formulae

1. Define (recursively) an interpretation function `intf : form -> Prop` that interprets every formula has its usual counterpart in the logic of Coq (`Tr` is interpreted by `True`, etc.) Atomic formulae are interpreted by themselves.

5.2 Soundness of the interpretation

1. Prove the for any derivation of $L \vdash A$ such that the interpretation of all assumptions of L hold, then the interpretation of A also holds.

5.3 Consistency of assumptions of HA

1. Prove that the interpretation of the assumptions of theories E and A hold.

5.4 Consistency of PA

1. Prove the consistency of PA (relative to the consistency of Coq)

$$\nvdash_{PA} \bot$$

by first reducing the consistency of PA to that of HA, and finally prove the consistency of HA by soundness of the interpretation and the reults of previous section.