

2.7.1 — Foundations of Proof Systems

Classroom exercises (TD)

Oct. 2nd 2023

1 Impredicative Definitions

Question 1 Give a definition of the property “being a power of 2” in HOL (that is that a number is some 2^i). \diamond

2 Cuts in HOL

2.1 Logical Cuts

Remember that in First-Order Logic (FOL) we have a notion of logical cut for each connector or quantifier, and each time a corresponding cut-elimination step. For instance

$$\frac{\frac{\frac{\sigma_A}{\vdash A} \quad \frac{\sigma_B}{\vdash B}}{\vdash A \wedge B}}{\vdash A} \quad \text{is simplified to} \quad \frac{\sigma_A}{\vdash A}.$$

In HOL however, the conjunction connector is not primitive but defined by :

$$A \wedge B \equiv \forall_o \lambda X^o. (A \Rightarrow B \Rightarrow X) \Rightarrow X.$$

Remark : In the following, I will sometimes write $\forall x^T \dots$ for $\forall_T \lambda X^T \dots$

Question 2 Write the proof derivation corresponding to the FOL logical cut above, when in HOL. \diamond

Question 3 Check whether this cut can be eliminated. That is whether the elimination of \forall and \Rightarrow cuts in HOL are sufficient for eliminating the \wedge cuts. \diamond

Question 4 Do the same for the disjunction in HOL. \diamond

2.2 Axiomatic Cuts

Question 5 Do the same for the axiomatic equality cut. Or, in other words, check whether the logical \forall and \Rightarrow cuts in HOL are sufficient to eliminate the axiomatic $=$ cuts. \diamond

At this stage, it is probably more useful to look at the Coq exercises; even for better understanding the next exercise. However, if you are not afraid you can look at the induction cuts below.

We now want to look at the axiomatic induction cuts. If we state the induction principle as an axiom, we will not be able to view the induction cuts as logical cuts. We can however slightly change the approach.

We first define a property over objects of type ι stating that they verify the induction principle :

$$\text{Nat} \equiv \lambda x^\iota. \forall_{\iota \rightarrow o} \lambda P^{\iota \rightarrow o}. (P\ 0) \implies (\forall n^\iota. (P\ n) \implies (P\ (S\ n))) \implies (P\ x).$$

We have $\text{Nat} : \iota \rightarrow o$. We can understand $(\text{Nat}\ n)$ as “ n is a natural number”.

Then, each time we quantify over a natural number, we add an assumption that it verifies Nat . So we can prove :

$$(1) \quad \forall n^\iota. (\text{Nat}\ n^\iota) \implies \exists p^\iota. n^\iota = r^\iota + r^\iota \vee n^\iota = S\ (r^\iota + r^\iota).$$

Question 6 Describe roughly how you prove, say, $(\text{Nat}\ 5)$. ◇

Question 7 Can you see what happens when you combine (1) with the result of the previous question to obtain a proof of $\exists p^\iota. 5 = r^\iota + r^\iota \vee 5 = S\ (r^\iota + r^\iota)$ and then eliminate the cuts? ◇