2.7.1 — Foundations of Proof Systems

Exam

Nov. 27th 2023

Durée de l'épreuve : 2 heures. Length of the exam : 2 hours.

1 HOL

For conciseness I write $\forall X^T. \dots$ instead of $(\forall_T\ \lambda X^T. \dots)$.

Question 1 Given two propositions A and B in HOL, what do the following propositions correspond to ? (in natural language)

1. $\forall X^o\,.\,A \implies X^o$
2. $\forall X^o\,.\,(A \implies B \implies X^o) \implies X^o$
3. $\forall X^o\,.\,(A \implies X^o) \implies X^o$
4. $\forall X^o\,.\,((A \implies B) \implies X^o) \implies ((B \implies A) \implies X^o) \implies X^o$ ◇

Question 2 Same question for the following constructions, given a property $P : \iota \to o$ and a relation $R : \iota \to \iota \to o$.

1. $\forall x^\iota.\forall y^\iota.(R\ x^\iota\ y^\iota) \implies (R\ y^\iota\ x^\iota) \implies \forall Q^{\iota\to o}\,.\,(Q\ x^\iota) \implies (Q\ y^\iota)$
2. $\forall X^o\,.\,(\forall x^\iota\,.\,(P\ x^\iota) \implies X^o) \implies X^o$
3. $\lambda a^\iota.\lambda b^\iota\,.\,\forall X^{\iota\to o}\,.\,(X^{\iota\to o}\ a^\iota) \implies (\forall x^\iota.\forall y^\iota.(X^{\iota\to o}\ x^\iota) \implies (R\ x^\iota\ y^\iota) \implies (X^{\iota\to o}\ y^\iota)) \implies (X^{\iota\to o}\ b^\iota)$ ◇

2 System F

We use the usual encoding of natural numbers in System F as Church Numerals of the following type :

$$\text{nat} \equiv \forall X\,.\,X \to (X \to X) \to X$$

Question 3 Define the type NN which encodes the pairs of natural numbers, as well as the corresponding terms :

$$\begin{aligned} \mathit{pair} &: \text{nat} \to \text{nat} \to NN \\ \pi_1 &: NN \to \text{nat} \\ \pi_2 &: NN \to \text{nat} \end{aligned}$$ ◇

Question 4 Define the term $s : NN \to NN$ corresponding to the function $(n, m) \mapsto (S\ n, n)$. ◇

Question 5 Use this to define a predecessor function over nat. ◇

3 Lists in Type Theory

We start not in Type Theory, but in System T, that is simply-typed λ-calculus with the constants :

$$\begin{array}{rcll} 0 & : & N & \\ S & : & N \to N & \\ R_T & : & T \to (N \to T \to T) \to N \to T & \text{(for any type } T\text{)} \end{array}$$

and the usual reduction rules for R_T.

Question 6 Extend this with corresponding constructions for a type list_T of lists whose elements are of type T with constants nil_T and $cons_T$. You can call RL_T the recursion operator over these lists. Give the corresponding reduction rules. ◇

Question 7 Transpose this to Martin-Löf's Type Theory (MLTT) by giving a dependent typing for this RL_T operator, so that it becomes an extension of MLTT. ◇

Independently, we extend MLTT with an operator $D : N \to \mathsf{Type}$ with two reduction rules :

$$\begin{array}{rcl} (D\ 0) & \rhd & \top \\ (D\ (S\ t)) & \rhd & \bot \end{array}$$

Question 8 Use this new operator to prove $0 =_N (S\ 0) \to \bot$ in this extension of MLTT.◇

Question 9 We now want to prove $\Pi x : T\ .\ \Pi l : \mathsf{list}_T\ .\ nil_T =_{\mathsf{list}_T} (cons_T\ x\ l) \to \bot$.

Do you need additional operator to prove this or can you do with the operator D of the previous question? How do you proceed? ◇

4 Surjective Pairing

One considers the following additional reduction rule for Martin-Löf's Type Theory :

$$(\pi_1(t), \pi_2(t)) \quad \rhd_{SR} \quad t$$

This reduction rule is know as the *surjective pairing* reduction. Note that the rule is not linear (the two occurrences of t in the left hand part need to be identical).

Question 10 Show that this rule enjoys the subject reduction property. That is, if $\Gamma \vdash (\pi_1(t), \pi_2(t)) : U$, then $\Gamma \vdash t : U$. ◇

5 Markov's Principle

In this section, we work in Martin-Löf's Type Theory (MLTT). We consider that P is a predicate over natural numbers, that is an object of type $N \to \mathsf{Type}$.

Question 11 Show that, for at least some values of P, the proposition $\neg\neg(\Sigma n : N.P\ n) \to \Sigma n : N.P\ n$ is not provable in MLTT. ◇

The soviet mathematician Andrei Markov proposed a version of this proposition, weakened in order to preserve constructivity. He suggested to admit the axiom $\neg\neg(\Sigma n : N.P\ n) \to \Sigma n : N.P\ n$ but only for decidable properties, that is provided the following is provable : $\forall n : N.P\ n + \neg(P\ n)$. (Here + denotes the sum type operator in MLTT).

In other words, Markov proposed to accept the following axiom scheme, which is thus known as *Markov's principle* :

$$(\forall n : N.P\ n + \neg(P\ n)) \to \neg\neg(\Sigma n : N.P\ n) \to \Sigma n : N.P\ n.$$

Question 12 Explain informally why Markov's principle can be constructive; that is how one could give evidence for Markov's principle in Heyting's semantics. ◇

(For the record, it is possible, but difficult, to show that Markov's principle is not provable in MLTT (or in Heyting's arithmetic).)

One proposes to extend MLTT with a specific term corresponding to Markov's principle in the Curry-Howard setting.

Given terms P, d, p, n, one has a new term $MP_P(d, p, n)$. One adds the following typing rule :

$$\frac{\Gamma \vdash P : N \to \mathsf{Type} \qquad \Gamma \vdash d : \forall n : N.P\ n + \neg(P\ n) \qquad \Gamma \vdash p : \neg\neg(\Sigma n : N.P\ n)}{\Gamma \vdash MP_P(d, p, 0) : \Sigma n : N.P\ n}$$

One suggests the following reduction rule :

$$(R_{MP}) \quad MP_P(d, p, n) \quad \triangleright \quad \delta(d\ n, x.(n\ x), y.MP_P(d, p, (S\ n)))$$

Remember δ is the elimination operator for sum types, that is logical disjunction.

Question 13 Explain the idea behind this *MP* operator and this reduction rule. ◇

Question 14 Show that this R_{MP} reduction rule is not strongly normalizable (or in other words, that MLTT with this reduction rule in not strongly normalizable). *This should be very short.* ◇

Question 15 Show that the system with the R_{MP} reduction rule is not weakly normalizable either. *Hint : you may look at the next question to find the idea.* ◇

One therefore suggests the following restriction : *the R_{MP} reduction can only be performed when the terms d and p are closed (that is they contain no free variable).*

Question 16 Sketch a proof of weak normalization for MLTT extended by this restricted R_{MP} reduction rule. ◇