2.7.1 — Foundations of Proof Systems

Exam

Nov. 26^{th} 2024

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

1 Exercises

1.1 Normal Terms

Question 1 If α, β are atomic type in simply typed λ-calculus. What are the closed normal terms of respective types :

- $\alpha \to \alpha$
- $\alpha \to \alpha \to \alpha$
- $(\beta \to \alpha) \to (\gamma \to \alpha) \to \beta \to \gamma \to \alpha$ ◇

Solution. $\lambda x^{\alpha}.x{\cdot}\alpha$
$\lambda x^{\alpha}.\lambda y^{\alpha}.x{\cdot}\alpha$ and $\lambda x^{\alpha}.\lambda y^{\alpha}.y{\cdot}\alpha$
$\lambda f.\lambda g.\lambda x.\lambda y.(f\ x)$ and $\lambda f.\lambda g.\lambda x.\lambda y.(g\ y)$ □

Question 2 In System F, what are the possible normal terms t of these respective types in these respective contexts :

- $[] \vdash t : \forall \alpha\ .\ \alpha \to \alpha$
- $[] \vdash t : \forall \alpha\ .\ \alpha \to \alpha \to \alpha$
- $[] \vdash t : \forall \alpha\ .\ \alpha$
- $[x : \alpha; y : \alpha] \vdash t : \alpha \to \alpha$ ◇

Solution. $\Lambda\alpha.\lambda x : \alpha.x$
$\Lambda\alpha.\lambda x : \alpha..\lambda y : \alpha.x$ and $\Lambda\alpha.\lambda x : \alpha..\lambda y : \alpha.y$
None
$\lambda z : \alpha.t$ where t is either x, y or z. □

Question 3 In Martin-Löf's type theory, what are the possible normal forms for terms t of these respective types in these respective contexts :

- $[] \vdash t : 4 =_N 4$
- $[] \vdash t : 3 + 2 =_N 5$
- $[] \vdash t : 3 =_N 2$

- $(t\ 4\ 5)$ where $[] \vdash t : \Pi a : N.\Pi b : N.\Sigma c : N.(a\ =_N\ (\mathsf{add}\ b\ c)) + (b\ =_N\ (\mathsf{add}\ a\ c))$. (where add is the definition of addition). ◇

Solution. $refl\ 4$
$refl\ 5$
none
$(1, j(refl 5))$ □

1.2 Constructivity

Question 4 Show that, given a propositional variable A, one can prove :

$$A \Rightarrow \neg\neg A$$

Question 5 Show that, given a propositional variable A, one can prove :

$$(A \vee \neg A) \Rightarrow (\neg\neg A \Rightarrow A).$$

(It is ok to describe the proof steps clearly instead of writing the full derivation.) ◇

Solution. Eliminate the assumption $A \vee \neg A$:

— If A, we have $\neg\neg A \Rightarrow A$.

— If $\neg A$, then $\neg\neg A$ implies false, and hence also A. □

Question 6 Explain why one cannot prove the reverse implication :

$$(\neg\neg A \Rightarrow A) \Rightarrow (A \vee \neg A).$$

Solution. Consider this implication by taking $\neg\neg B$ for A. When then can show $A \Rightarrow \neg\neg A$ (since $\neg\neg\neg C \Rightarrow \neg C$ for any C. So we would have a way to decide whether any proposition is false or not false ; which is undecidable. □

1.3 Que j'itère

We are in the Calculus of Constructions. We recall the way to code natural numbers :

$$\begin{aligned} \text{nat} &\equiv \Pi X : \mathsf{Type}.X \to (X \to X) \to X \\ 0 &\equiv \lambda X : \mathsf{Type}.\lambda x : X.\lambda f : X \to X.x \\ S &\equiv \lambda n : \text{nat}\,.\lambda X : \mathsf{Type}.\lambda x : X.(f\ (n\ X\ x\ f)) \end{aligned}$$

One will write 1, 2, *etc* for $(S\ 0), (S\ (S\ 0)) \ldots$ One also assumes that addition and multiplication have been defined.

One defines :

$$\mathsf{myst} \equiv \lambda n : \text{nat}\,.\Pi P : \text{nat} \to \mathsf{Type}.(P\ 1) \to (\Pi x : \text{nat}\,.(P\ x) \to (P\ (\mathsf{mult}\ 2\ x))) \to (P\ n)$$

Question 7 What is the type of myst ? ◇

Solution. $\mathsf{nat} \to \mathsf{Type}$ □

Question 8 Give Proof terms for ($\mathsf{myst}\ 1$) and ($\mathsf{myst}\ 2$). ◇

Solution. $\lambda P.\lambda p_1 : (P\ 1).\lambda p_2 : \Pi x : \mathsf{nat}\,.(P\ x) \to (P\ (\mathsf{mult}\ 2\ x)).p_1$
$\lambda P.\lambda p_1 : (P\ 1).\lambda p_2 : \Pi x : \mathsf{nat}\,.(P\ x) \to (P\ (\mathsf{mult}\ 2\ x)).(p_2\ 1\ p_1)$ □

Question 9 What is the mathematical "meaning" of ($\mathsf{myst}\ n$) (in regular mathematical language)? ◇

Solution. There exists a natural i, such that $n = 2^i$. □

Question 10 One wants a term

$$div2 : \Pi n : \mathsf{nat}\,.(\mathsf{myst}\ n) \to \mathsf{nat}$$

such that ($div2\ n\ p$) reduces to $log_2(n)$. Give such a (as simple as possible) term $div2$ (we here mean the original definition of myst. ◇

Solution.

$$div2 \equiv \lambda n.\lambda p : (\mathsf{myst}\ n).(p\ (\lambda x : \mathsf{nat}\,.\mathsf{Type})\ 0\ \lambda x : \mathsf{nat}\,.\lambda y : \mathsf{nat}\,.(S\ y)$$

2 Type System with ordinals

In this section we consider an extension of System T (and thus of MLTT) with a form of ordinals.

— One adds a new type ord to the system (thus with a rule $[] \vdash \mathsf{ord} : \mathsf{Type}$)

— this type has three constructors :

  — $0_o : \mathsf{ord}$

  — $\mathsf{S}_o : \mathsf{ord} \to \mathsf{ord}$

  — $\mathsf{lim} : (N \to \mathsf{ord}) \to \mathsf{ord}$ (N is the usual type of naturals in system T, which comes with its own family of recursors R^T as studied in the course).

and one recursor over ord for any target type T :

$$\frac{\Gamma \vdash T : \mathsf{Type}}{\mathsf{R}^{ord}{}_T : T \to (\mathsf{ord} \to T \to T) \to ((N \to \mathsf{ord}) \to (N \to T) \to T) \to \mathsf{ord} \to T}$$

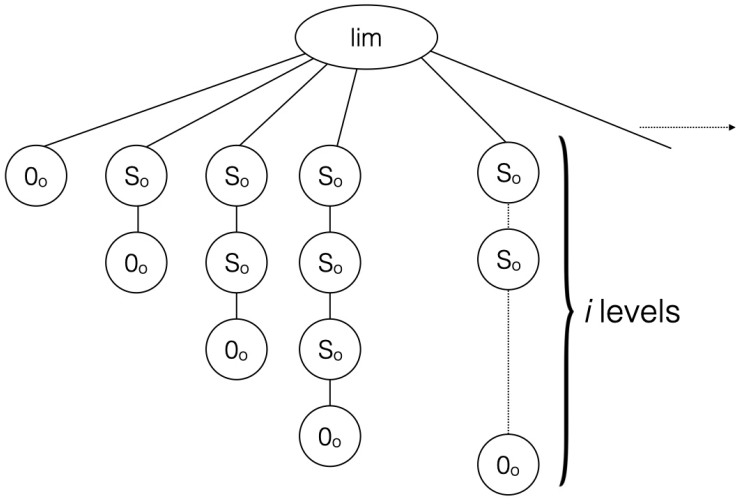
with the following reduction rules :

1. $\mathsf{R}^{ord}{}_T\ t_0\ t_S\ t_l\ 0_o \rhd t_0$
2. $\mathsf{R}^{ord}{}_T\ t_0\ t_S\ t_l\ (\mathsf{S}_o\ o) \rhd t_S\ o\ (\mathsf{R}^{ord}{}_T\ t_0\ t_S\ t_l\ o)$
3. $\mathsf{R}^{ord}{}_T\ t_0\ t_S\ t_l\ (\mathsf{lim}\ f) \rhd t_l\ f\ \lambda n : N.(\mathsf{R}^{ord}{}_T\ t_0\ t_S\ t_l\ (f\ n))$

Question 11 Define the straightforward injection $\mathsf{N\_\ to\_\ ord}$ of type $N \to \mathsf{ord}$. ◇

Solution. `Definition nat_to_ord := R ord Oo (fun p r => So r).`

Note that the elements of type ord can be seen as infinitely branching trees. For instance the element (lim N_ to_ ord) can be drawn as :



Question 12 Define a function r : ord $\to N$ such that, for any closed $n : N$, one has $(r\ (\mathsf{N\_\ to\_\ ord}\ n)) \rhd n$. ◇

Solution.
```
Definition r :=
  Ro nat 0 (fun _ xr => (S xr))
     (fun _ _ => 0).
```

Question 13 How can you encode the type ord using the impredicative encoding in System F? Give the definitions of ord, 0_o and S_o. ◇

Solution.

$$\forall\alpha.\alpha \to (\alpha \to \alpha) \to ((N \to \alpha) \to \alpha) \to \alpha$$

$$\Lambda\alpha.\lambda x : \alpha.\lambda f : \alpha \to \alpha.\lambda l : (N \to \alpha) \to \alpha.x$$

$$\lambda o : \mathsf{ord}.\Lambda\alpha.\lambda x : \alpha.\lambda f : \alpha \to \alpha.\lambda l : (N \to \alpha) \to \alpha.f\ (o\ \alpha\ x\ f\ l)$$

$$\lambda g : N \to \mathsf{ord}.\Lambda\alpha.\lambda x : \alpha.\lambda f : \alpha \to \alpha.\lambda l : (N \to \alpha) \to \alpha.l\ \lambda n : N.(o\ \alpha\ x\ f\ l)$$

Question 14 Give the typing of the R^{ord} operator(s) in MLTT (that is the version with dependent types). ◇

Solution.

$$\frac{\Gamma \vdash P : \mathsf{ord} \to \mathsf{Type}}{\begin{array}{l}\mathsf{R}^{ord}{}_P : (P\ 0_o) \to \\ \quad (\Pi x : \mathsf{ord}.(P\ x) \to (P\ (\mathsf{S}_o\ x)) \to \\ \quad\quad (\Pi u : N \to \mathsf{ord}(\Pi n : N.P\ (u\ n)) \to \\ \quad\quad (P\ (\mathsf{lim}\ u))) \to \\ \quad\quad\quad \Pi x : \mathsf{ord}.P\ x\end{array}}$$

Question 15 In this extension of MLTT, show hot to prove

$$\Pi n : N.(r\ (\mathsf{N\_\ to\_\ ord}\ n))\ =_N\ n.$$

(The two functions are the ones defined in questions 11 and 12. Please do not go into too much detail ; just give the main steps of the proof construction). ◇

Solution. Simple induction over n, doing some β-reduction of the proposition in each case. □

Strong Normalization

We want to prove strong normalization for this extension of System T (we thus do not need to consider dependent types in this part).

In order to explain the technique, we start by modifying the normalization proof for regular System T, by changing the definition of the reducibility set $|N|$ (which is $|T| \equiv \mathcal{SN}$ in the "usual" proof).

Like in System F, we define reducibility candidates :

Définition 1 We call $\mathcal{SN}$ the set of strongly normalizing terms. The set $\mathcal{N}$ of neutral terms is the set of terms which are not of one of the following forms : $\lambda x^T.t, 0, (S\ t)$. ◇

Définition 2 A set C of λ-terms is said to be a reducibility candidate ($C \in \mathcal{CR}$) if and only if these three conditions are verified :

1. $C \subseteq \mathcal{SN}$,
2. $\forall t \in C, t \rhd_\beta t' \Rightarrow t' \in C$,
3. $\forall t \in \mathcal{N}, (\forall t', t \rhd t' \Rightarrow t' \in C) \Rightarrow t \in C$. ◇

Given two sets of terms X and Y one defines :

$$X \to Y \equiv \{t \mid \forall u \in X, (t\ u) \in Y\}.$$

We recall the two facts which you do not have to show :

— If X and Y are reducibility candidates, then $X \to Y$ is a reducibility candidate.

— If $(C_i)_{i\in I}$ is a family of reducibility candidates (resp. $A \subset \mathcal{CR}$) then $\bigcap_{i\in I} C_i \in \mathcal{CR}$ (resp. $\bigcap A \in \mathcal{CR}$).

In the new proof, we define $|N|$ as the smallest reducibility candidate such that, for any reducibility candidate X, we have :

$$(1)\ \ t \in |N| \Leftrightarrow \forall t_0 \in X, \forall t_S \in |N| \to X \to X, (R\ t_0\ t_S\ t) \in X.$$

The two next questions are to show that this set exists ; they may be skipped in the first run.

Question 16 Given sets of terms X and C we define

$$F(C, X) \equiv \{t \mid \forall t_0 \in X, \forall t_S \in C \to X \to X, \quad (R\ t_0\ t_S\ t) \in X\}.$$

Show that for any C and C', $C \subseteq C' \Rightarrow F(C) \subseteq F(C')$.

Deduce that $\bigcap_{X\in\mathcal{CR}} F(C, X) \subset \bigcap_{X\in\mathcal{CR}} F(C', X)$ ◇

Solution. We first show that : if $C \subseteq C'$ then $C' \to A \subset C \to A$. If $t \in C' \to A$, then any $u \in C$ is also element of C' and thus $t\ u \in A$.

Let $t \in F(C, X)$. To show that $t \in F(C', X)$ we consider $t_0 \in X$ ad $t_S \in C' \to X \to X$.

We thus know that $t_S \in C \to X \to X$, and it follows from the definition that $R\ t_0\ t_S\ t \in X$. Qed.

The second step is also basically simple (the $\bigcap$ operator is covariant) □

Question 17 Show that, if C and X are reducibility candidates, then $F(C, X)$ is a reducibility candidate.

Deduce that, if C is a reducibility candidate, $\bigcap_{X \in \mathcal{CR}} F(C, X)$ is a reducibility candidate. ⋄

Solution. (1) If C and X are RC, then so is $C \to X \to X$. So there exists SN terms $t_0 \in X$ and $t_S \in C \to X \to X$.

So $(R\ t_0\ t_S\ t) \in X \subseteq \mathcal{SN}$, so $t \in \mathcal{SN}$.

(2) If $(R\ t_0\ t_S\ t) \in X$ and $t \triangleright t'$, then $(R\ t_0\ t_S\ t') \in X$ (because X verifies (2)). So $t' \in F(C, X)$.

(3) If $t \in \mathcal{N}$ and $(R\ t_0\ t_S\ t) \in X$ and $\forall t', t \triangleright t' \Rightarrow t' \in F(C, X)$ then

$$\forall t', t \triangleright t' \Rightarrow (R\ t_0\ t_S\ t) \in X$$

we can show by induction over the length of the possible reduction paths from t_0 and t_S that $(R\ t_0\ t_S\ t) \in X$.

The key is that reducts of $(R\ t_0\ t_S\ t)$ are of one of the forms $(R\ t'_0\ t_S\ t)$, $(R\ t_0\ t'_S\ t)$, $(R\ t_0\ t_S\ t')$.

Now, since for any $X \in \mathcal{CR}$, $F(C, X)$ is a $\mathcal{CR}$, the intersection $\bigcap_{X \in \mathcal{CR}} F(C, X)$ is a $\mathcal{CR}$.

We then write $G(C) \equiv \bigcap_{X \in \mathcal{CR}} F(C, X)$. We can then define :

$$|N| \equiv \bigcap \{C \in \mathcal{CR} \mid G(C) \subseteq G\}$$

which verifies condition (1).

Question 18 Show that $0 \in |N|$ and $S \in |N| \to |N|$. ⋄

Solution. We show that $0 \in |N|$. For that, we consider $\mathcal{C} \in \mathcal{CR}$ s.t. $G(C) \subseteq G$ and show that $O \in \mathcal{C}$.

That is, given $X \in \mathcal{CR}$ we show that $O \in F(C, X)$

That is, given $t_O \in X$ and $t_S \in C \to X \to X$ we show that $(R\ t_0\ t_S\ 0) \in X$.

The reducts of $(R\ t_0\ t_S\ 0)$ are either :

— t_0 which is in X

— $(R\ t'_0\ t_S\ 0)$ or $(R\ t_0\ t'_S\ 0)$ which can be shown being in X by the now usual induction.

The case of S is similar. □

Question 19 Show that if, for some type T, $t_0 \in |T|$ and $t_0 \in |N| \to |T| \to |T|$ and $t \in |N|$, then $(R_T\ t_0\ t_S\ t) \in |T|$. ⋄

Question 20 Following the construction above, how can you define the reducibility set $|\mathsf{ord}|$? Roughly describe the steps of the strong normalization proof. ⋄

Solution. We adapt the definition of $\mathcal{N}$ (and thus of $\mathcal{CR}$ saying that 0_o, $(\mathsf{S}_o\ t)$ and $(\mathsf{lim}\ f)$ are not neutral.

Then we take $|\mathsf{ord}|$ as the smallest reducibility candidate such that, for any $X \in \mathcal{CR}$

$$t \in |\mathsf{ord}| \Leftrightarrow \forall t_0 \in X, \forall t_S \in |\mathsf{ord}| \to X \to X, \forall t_l \in (|N| \to |ord|) \to (|N| \to X) \to X, (\mathsf{R}^{ord}\ t_0\ t_S\ t_l\ t) \in X.$$

One then shows, like above, that $0_o, \mathsf{S}_o, \mathsf{lim}$ and R^{ord} belong to the correct reducibility set (like in the questions above for N).

This example shows that, for complex inductive types, we construct the reducibility interpretation inductively (in Set Theory). □