

Foundations of Proof Systems

Exercises

Sept. 25th 2026

1 System T

We recall System T is simply-typed λ -calculus with the constants :

$$\begin{aligned} 0 & : N \\ S & : N \rightarrow N \\ R_T & : T \rightarrow (N \rightarrow T \rightarrow T) \rightarrow N \rightarrow T \quad (\text{for any type } T) \end{aligned}$$

and the usual reduction rules for R_T .

Question 1 Define addition and multiplication in T.

Solution.

$$\begin{aligned} add & \equiv \lambda n^N. \lambda m^N. (R_N m^N \lambda p^N. \lambda r^N. S(r) n^N) \\ mul & \equiv \lambda n^N. \lambda m^N. (R_N 0 \lambda p^N. \lambda r^N. (add r n^N) n^N) \end{aligned}$$

Question 2 Define Ackermann's function in System T, that is a function of type $N \rightarrow N \rightarrow N$ such that :

$$\begin{aligned} A \ 0 \ m & = S(m) \\ A \ S(n) \ 0 & = A \ n \ S(0) \\ A \ S(n) \ S(m) & = A \ n \ (A \ S(n) \ m) \end{aligned}$$

◇

Solution. One uses two nested occurrences of the recursor. The outer one is $R_{N \rightarrow N}$ which defines $(A \ n)$ by structural recursion over n .

$$A \equiv (R_{N \rightarrow N} \lambda x^N. S(x^N) \lambda p^n. \lambda f^{N \rightarrow N}. (R_N (f \ 1) (\lambda p'^N. \lambda r^n. (f \ r))))$$

Or equivalently :

$$A \equiv \lambda n^N. \lambda m^N. (R_{N \rightarrow N} \lambda x^N. S(x^N) \lambda p^n. \lambda f^{N \rightarrow N}. (R_N (f \ 1) (\lambda p'^N. \lambda r^n. (f \ r))) \ n \ m).$$

Or in Rocq :

```

Definition R :=
  fun (T : Type) (t0 : T) (tS : nat -> T -> T) (n : nat) =>
    nat_rect (fun _ : nat => T) t0 tS n.

```

```

Definition Ack n m :=
  (R (nat->nat) S
    (fun _ (fr : nat -> nat) =>
      (R nat (fr 1)
        (fun _ r => fr r)))) n m).

```

2 Deduction Modulo

Let P and Q be two proposition symbols (that is two predicate symbols of arity 0) and consider the theory in Deduction modulo theory, formed with the rewrite rule

$$P \longrightarrow (P \Rightarrow Q)$$

Question 3 Give a proof of Q in this theory ◇

Solution.

$$\begin{array}{c}
 \frac{}{P \vdash P} \text{Ax} \quad \frac{}{P \vdash P \Rightarrow Q} \text{Ax} \quad \frac{}{P \vdash P} \text{Ax} \quad \frac{}{P \vdash P \Rightarrow Q} \text{Ax} \\
 \hline
 \frac{}{P \vdash Q} \Rightarrow\text{-I} \quad \frac{}{P \vdash Q} \Rightarrow\text{-I} \\
 \hline
 \frac{}{\vdash P \Rightarrow Q} \Rightarrow\text{-E} \quad \frac{}{\vdash P} \Rightarrow\text{-E} \\
 \hline
 \vdash Q
 \end{array}$$

We use the conversion three times : in two axiom rules to deduce $P \longrightarrow Q$ from hypothesis P , and in the right hand $\Rightarrow\text{-I}$ rule, to go from $P \vdash Q$ to $\vdash P$.

Notice that, the λ -term corresponding to this derivation is $(\lambda x^P.(x^P x^P) \lambda x^P.(x^P x^P))$, which becomes typable if one adds a rule $P = P \rightarrow Q$ to simple types.

Obviously, this derivation is not cut-free. □

Question 4 Does this proposition have a cut-free proof? ◇

Solution. Although this theory modulo cannot be mapped to simply typed λ -calculus for proving cut elimination, we see that if some proposition A is convertible to some $B \Rightarrow C$, then either A is atomic (for instance $A = P$) or $A = B' \Rightarrow C'$ with B and B' (resp. C and C' convertible).

So we know that a cut-free derivation of $\vdash Q$ must end with an introduction rule. This cannot be the case, because Q is not convertible to any $R_1 \Rightarrow R_2$.

So there is no cut-free proof of $\vdash Q$. □

3 Heyting Arithmetic

Question 5 Can one prove in HA

$$\forall x. \exists y. x = y + y \vee x = S(y + y) \quad ?$$

What may the cut-free proof end with? ◇

Solution. It is possible and is proved by induction over x . So the proof will and by the induction axiom, applied to two proofs of :

$$\begin{aligned} \exists y. 0 = y + y \vee 0 = S(y + y) \\ \forall x. (\exists y. x = y + y \vee x = S(y + y)) \Rightarrow \exists y. S(x) = y + y \vee S(x) = S(y + y) \end{aligned}$$

Question 6 Consider a cut-free proof of the following consequence of this proposition :

$$\exists y. 6 = y + y \vee 6 = S(y + y).$$

How does the proof end? Can you give the full proof? ◇

The proof will end with an introduction of existential, where the “witness” is 3.

More precisely, the full proof will be :

$$\frac{\frac{\frac{\vdash \forall x. x=x}{\vdash 6=3+3} A_x}{\vdash 6=3+3 \vee 6=S(3+3)} \vee\text{-I}_1}{\vdash \exists y. 6=y+y \vee 6=S(y+y)} \exists\text{-I}$$