

answers to the exam logical verification of January 18, 2006

1a

$$\frac{[A \rightarrow A \rightarrow B^x] \quad \frac{[C \rightarrow A^y] \quad [C^z]}{A} E \rightarrow}{A \rightarrow B} E \rightarrow \quad \frac{[C \rightarrow A^y] \quad [C^z]}{A} E \rightarrow}{\frac{B}{C \rightarrow B} I[z] \rightarrow \quad \frac{(C \rightarrow A) \rightarrow C \rightarrow B}{(A \rightarrow A \rightarrow B) \rightarrow (C \rightarrow A) \rightarrow C \rightarrow B} I[y] \rightarrow} I[x] \rightarrow$$

1b

We use the following:

$$\Gamma_0 = \{x : A \rightarrow A \rightarrow B\}$$

$$\Gamma_1 = \{x : A \rightarrow A \rightarrow B, y : C \rightarrow A\}$$

$$\Gamma_2 = \{x : A \rightarrow A \rightarrow B, y : C \rightarrow A, z : C\}$$

$$\frac{\Gamma_2 \vdash x : A \rightarrow A \rightarrow B \quad \frac{\Gamma_2 \vdash y : C \rightarrow A \quad \Gamma_2 \vdash z : C}{\Gamma_2 \vdash (yz) : A}}{\Gamma_2 \vdash x(yz) : A \rightarrow B} \quad \frac{\Gamma_2 \vdash y : C \rightarrow A \quad \Gamma_2 \vdash z : C}{\Gamma_2 \vdash (yz) : A}}{\frac{\Gamma_2 \vdash x(yz)(yz) : B}{\Gamma_1 \vdash \lambda z : C. x(yz)(yz) : C \rightarrow B}}{\Gamma_0 \vdash \lambda y : C \rightarrow A. \lambda z : C. x(yz)(yz) : (C \rightarrow A) \rightarrow C \rightarrow B}}{\vdash \lambda x : A \rightarrow A \rightarrow B. \lambda y : C \rightarrow A. \lambda z : C. x(yz)(yz) : (A \rightarrow A \rightarrow B) \rightarrow (C \rightarrow A) \rightarrow C \rightarrow B}$$

1c

$$\lambda z : A. \lambda y : B. (\lambda x : A. y) z$$

$$(\lambda x : A \rightarrow (A \rightarrow B) \rightarrow B. x) (\lambda y : A. \lambda z : A \rightarrow B. z y)$$

$$\lambda x : A \rightarrow A. \lambda y : A. \lambda z : B. x(x y)$$

1d

$$\frac{[B^y] \quad \frac{[A^x]}{B \rightarrow A} I[z] \rightarrow}{E \rightarrow} \quad \frac{A}{B \rightarrow A} I[y] \rightarrow}{A \rightarrow B \rightarrow A} I[x] \rightarrow$$

The first two steps (reading downwards) for a detour.

2a

```
Inductive natlist : Set :=
| nil : natlist
| cons : nat -> natlist -> natlist .
```

2b

```
natlist_ind
  : forall P : natlist -> Prop,
    P nil ->
    (forall (n : nat) (n0 : natlist),
     P n0 -> P (cons n n0)) ->
    forall n : natlist, P n
```

2c

For

```
Inductive le (n : nat) : nat -> Prop :=
| le_n : le n n
| le_S : forall m : nat, le n m -> le n (S m) .
```

we have the following:

- $\text{le_n } 0$ is an inhabitant of $\text{le } 0 \ 0$.
- there is no inhabitant of $\text{le } (S \ 0) \ 0$; intuitively because we do not have $1 \leq 0$.
- $(\text{le_S } 0 \ 0 \ (\text{le_n } 0))$ is an inhabitant of $\text{le } 0 \ (S \ 0)$.

2d

```
Inductive lelist : nat -> natlist -> Prop :=
| lelist_nil : forall n:nat, lelist n nil
| lelist_cons : forall n:nat, forall h:nat, forall t:natlist,
  le n h -> lelist n (cons h t) .
```

an alternative:

```
Definition lelist_b (n:nat) (l:natlist): Prop :=
match l with
| nil => True
| cons m l => (le n m)
end.
```

3a

the introduction \rightarrow immediately followed by the elimination \rightarrow :

$$\frac{\frac{B}{A \rightarrow B} I[x] \rightarrow \quad A}{B} E \rightarrow$$

the introduction \forall immediately followed by the elimination \forall :

$$\frac{\frac{A}{\forall x. A} I \forall \quad A[x := M]}{A[x := M]} E \forall$$

3b

$$\frac{[(\forall x. P(x)) \vee (\forall x. Q(x))]^a \quad \frac{\frac{\frac{[\forall x. P(x)]^b}{P(x)} E \forall \quad I \forall}{P(x) \vee Q(x)} I \vee \quad (\forall x. P(x)) \rightarrow (P(x) \vee Q(x))}{(\forall x. P(x)) \rightarrow (P(x) \vee Q(x))} I[b] \rightarrow \quad \frac{\frac{\frac{[\forall x. Q(x)]^c}{Q(x)} E \forall \quad I \forall}{P(x) \vee Q(x)} I \vee \quad (\forall x. Q(x)) \rightarrow (P(x) \vee Q(x))}{(\forall x. Q(x)) \rightarrow (P(x) \vee Q(x))} I[c] \rightarrow}{\frac{P(x) \vee Q(x)}{\forall x. (P(x) \vee Q(x))} I \forall \quad ((\forall x. P(x)) \vee (\forall x. Q(x))) \rightarrow \forall x. (P(x) \vee Q(x))} I[a] \rightarrow} E \exists$$

4a `natlist_dep` has type `nat \rightarrow *`

4b `nat \rightarrow * : \square`

4c `nil_dep : natlist_dep 0`

4d

Definition `length_dep (n : nat) (l : natlist_dep n) := n.`

an alternative:

```
Definition length_dep_b (n : nat) (l : natlist_dep n) : nat :=
  match l with
  | nil_dep => 0
  | cons_dep n h t => S n
  end.
```

5a The type checking problem: given a term P , a type A , and an environment Γ , do we have $\Gamma \vdash P : A$?

5b The proof checking problem: given a proof P with assumptions Γ , and a formula A , is P a proof of A ?

5c For instance, the atomic type A is not inhabited by a closed λ -term. Also, the simple type $A \rightarrow B$ with A and B atomic types is not inhabited by a closed λ -term.

6a

$$\frac{\frac{[a^x]}{a \rightarrow a} I[x]}{\forall a. a \rightarrow a} I\forall \rightarrow$$

6b $\Pi a:*. a \rightarrow a$

6c The polymorphic identity: $\lambda a:*. \lambda x:a. x$

6d

$$\frac{\vdash *: \square}{a : * \vdash a : *}$$

6e

$$\frac{\frac{6d}{a : *, x : a \vdash x : a} \quad \frac{6d \quad \frac{6d \quad 6d}{a : *, x : a \vdash a : *}}{a : * \vdash a \rightarrow a : *}}{a : * \vdash \lambda x:a. x : a \rightarrow a}$$

6f

$$6e \quad \frac{\frac{\frac{6d \quad \frac{6d \quad 6d}{a : *, x : a \vdash a : *}}{a : * \vdash a \rightarrow a : *} \quad \vdash *: \square}{\vdash \Pi a:*. a \rightarrow a : *}}{\lambda a:*. \lambda x:a. x : \Pi a:*. a \rightarrow a}$$