Université de Strasbourg
Ingénierie de la preuve Feuille de CT (Correction)

Examen Mai 2010

Notes de cours manuscrites autorisées. Le barème est donné à titre indicatif.

Logique et Isomorphisme de Curry-Howard (7 points)

1. (a) Proposer une preuve en déduction naturelle de la proposition suivante :

$$\forall ABC, ((A \Rightarrow B) \Rightarrow (A \Rightarrow C)) \Rightarrow (A \Rightarrow B) \Rightarrow A \Rightarrow C$$

Correction :

(b) Donner la preuve de cette proposition sous forme d'une suite de tactiques Coq.
Correction : Première solution :

```
Lemma q1: forall A B C : Prop,
  ((A -> B) -> (A -> C)) ->
   (A -> B) -> A -> C.
Proof.
intros A B C H1 H2 .
apply (H1 H2).
Qed.
```

Deuxième solution :

```
Lemma q1: forall A B C : Prop,
  ((A -> B) -> (A -> C)) ->
   (A -> B) -> A -> C.
Proof.
intros A B C H1 H2 H3.
apply H1.
apply H2.
apply H3.
Qed.
```

(c) Donner le terme de preuve correspondant.
Correction : Première solution :

```
fun (A B C : Prop) (H1 : (A -> B) -> A -> C)
                   (H2 : A -> B) => H1 H2
```

Deuxième solution :

```
fun (A B C : Prop) (H1 : (A -> B) -> A -> C)
                   (H2 : A -> B)
                   (H3 : A) => H1 H2 H3
```

2. (a) Proposer une preuve en déduction naturelle de la proposition suivante :

$$\forall AB, A \wedge B \Rightarrow A \wedge (A \vee B)$$

Correction :

(b) Donner la preuve de cette proposition sous forme d'une suite de tactiques Coq.
Correction :

```
Lemma q2: forall A B: Prop, A /\ B  -> A /\ (A \/ B).
Proof.
intros A B HAB.
split.
elim HAB.
intros HA HB.
assumption.
left.
elim HAB.
intros HA HB.
assumption.
Qed.
```

(c) Donner le terme de preuve correspondant.
Correction :

```
fun (A B : Prop) (HAB : A /\ B) =>
conj (and_ind (fun (HA : A) (HB : B) => HA) HAB)
  (or_introl B (and_ind (fun (HA : A) (HB : B) => HA) HAB))
```

3. Soit le terme de preuve suivant :

```
fun (A B C : Prop) (H1 : (C -> B) -> A -> C)
                   (H2 : A -> C -> B)
                   (H3 : A) => H1 (H2 H3) H3
```

De quelle formule est-il la preuve ?
Correction :

```
forall A B C : Prop, ((C -> B) -> A -> C) -> (A -> C -> B) -> A -> C
```

Preuve par réccurence (5 points)

On considère la fonction suivante :

```
Fixpoint mult2 (n:nat) : nat :=
  match n with
    O => O
  | (S p) => (S (S (mult2 p)))
  end.
```

1. Ecrire les règles de calcul associées à cette définition. On rappelle que les règles demandées sont celles qui s'appliquent lors de l'appel à la tactique `simpl`.
Correction :

```
mult2 O -> 0
mult2 (S p) -> S (S (mult2 p))
```

2. Donner la preuve Coq du lemme suivant (en précisant le but à prouver aux différentes étapes) :

```
Lemma mult2_plus: forall n: nat, mult2 n = n + n.
```

Indication : on posera un lemme intermediaire.

Correction :

On procède par induction sur n.

Pour le cas de base 0 il faut montrer que : `mult2 0 = 0 + 0`. Après simplification on obtient : `0 = 0`.

Pour le cas d'induction on doit prouver que : `mult2 (S n) = S n + S n` en sachant que `mult2 n = n + n`. D'après les règles de réduction de `mult2` on a : `S (S (mult2 n)) = S n + S n`. D'après l'hypothèse de réccurence il faut donc prouver que : `S (S (n + n)) = S n + S n`. C'est le lemme que l'on peut poser.

```
Lemma SS_plus : forall n m,
  S (S (n+m)) = S n + S m.
Proof.
intros.
induction n.
simpl; reflexivity.
simpl.
rewrite IHn.
reflexivity.
Qed.

Lemma exo2a: forall n: nat, mult2 n = n + n.
Proof.
intros.
induction n.
simpl.
reflexivity.
replace (mult2 (S n)) with (S (S (mult2 n))) by trivial.
rewrite IHn.
apply SS_plus.
Qed.
```

Autre solution on simplifie un peu plus et on pose un lemme un peu différent :

```
Lemma S_plus : forall n m,
  S (n+m) = n + S m.
Proof.
intros.
induction n.
simpl; reflexivity.
simpl.
rewrite IHn.
reflexivity.
Qed.

Lemma exo2b: forall n: nat, mult2 n = n + n.
Proof.
intros.
induction n.
simpl.
reflexivity.
simpl.
rewrite IHn.
rewrite S_plus.
```

```
reflexivity.
Qed.
```

Jeu des allumettes (8 points)

On dispose d'un nombre n d'allumettes ($n > 0$) sur une table. Les joueurs A et B jouent chacun leur tour et peuvent retirer de 1 à 3 allumettes de la table. Le joueur qui retire la dernière allumette a gagné.

Exemple de partie :

On dispose 12 allumettes. C'est au joueur A de commencer.

1. Le joueur A retire 2 allumettes, il en reste 10
2. Le joueur B retire 1 allumettes, il en reste 9
3. Le joueur A retire 3 allumettes, il en reste 6
4. Le joueur B retire 2 allumettes, il en reste 4
5. Le joueur A retire 2 allumettes, il en reste 2
6. Le joueur B retire 2 allumettes, il n'en reste plus, le joueur B a gagné.

Nous allons définir un prédicat inductif qui modélise ce jeu. Soit J l'ensemble des joueurs qui contient seulement deux éléments : A et B. Nous souhaitons définir un prédicat $G(X, Y, n)$ qui signifie que le joueur X peut gagner de façon sûre si c'est au joueur Y de jouer et qu'il reste n allumettes sur la table. Par exemple la formule $G(A, B, 4)$ signifie que le joueur A peut gagner de façon sûre si c'est au joueur B de jouer et qu'il reste 4 allumettes sur la table.

Considérons la première définition inductive suivante :

Axiomes :

$$\frac{}{G(A,B,4)} \quad \frac{}{G(B,A,4)}$$

Règles :

$$\frac{G(A,B,n)}{G(A,A,n+1)} \quad \frac{G(A,B,n)}{G(A,A,n+2)} \quad \frac{G(A,B,n)}{G(A,A,n+3)} \quad \frac{G(A,B,n)}{G(A,B,n+4)}$$

$$\frac{G(B,A,n)}{G(B,B,n+1)} \quad \frac{G(B,A,n)}{G(B,B,n+2)} \quad \frac{G(B,A,n)}{G(B,B,n+3)} \quad \frac{G(B,A,n)}{G(B,A,n+4)}$$

1. Proposer un type inductif `joueur` permettant de représenter l'ensemble des joueurs.
   Correction :

```
Inductive joueur : Set :=
  A : joueur
| B : joueur.
```

2. Définir en Coq un prédicat inductif `sys_g_1` de type `joueur -> joueur -> nat -> Prop` qui correspond à la définition inductive donnée ci-dessus.
   Correction :

```
Inductive sys_g_1 : joueur -> joueur -> nat -> Prop :=
| A1a : sys_g_1 A B 4
| A1b : sys_g_1 B A 4
| R1a : forall n, sys_g_1 A B n ->  sys_g_1 A A (n+1)
| R2a : forall n, sys_g_1 A B n ->  sys_g_1 A A (n+2)
| R3a : forall n, sys_g_1 A B n ->  sys_g_1 A A (n+3)
| R4a : forall n, sys_g_1 A B n ->  sys_g_1 A B (n+4)
| R1b : forall n, sys_g_1 B A n ->  sys_g_1 B B (n+1)
| R2b : forall n, sys_g_1 B A n ->  sys_g_1 B B (n+2)
| R3b : forall n, sys_g_1 B A n ->  sys_g_1 B B (n+3)
| R4b : forall n, sys_g_1 B A n ->  sys_g_1 B A (n+4)
.
```

3. Donner la preuve en Coq de fait que `sys_g_1 A A 5`.
   Correction :

```
Lemma l1 : sys_g_1 A A 5.
Proof.
replace 5 with (4+1) by (simpl;reflexivity).
(*
1 subgoal
_____________________________________(1/1)
sys_g_1 A A (4 + 1)
*)
apply R1a.
(*
1 subgoal
_____________________________________(1/1)
sys_g_1 A B 4
*)
apply A1a.
Qed.
```

4. Donner l'idée de la preuve en Coq (aussi précise que possible) du lemme suivant, quels lemmes sont nécessaires ?

   `Lemma sys_g_1_n_4 : forall X Y n, sys_g_1 X Y n -> n>=4.`

   Correction : On fait une preuve par induction. Pour les deux cas de base correspondant aux axiomes il suffit de montrer que `4>=4`. Pour les autres cas il faut montrer que `n >= 4 -> n+1 >= 4`, `n >= 4 -> n+2 >= 4`.... Pour information, ces différents lemmes se prouvent à l'aide de la tactique omega (mais cette information n'avait pas à être donnée).

```
Lemma sys_g_1_n_4 : forall X Y n, sys_g_1 X Y n -> n>=4.
Proof.
intros X Y n H.
induction H;omega.
Qed.
```

5. Donner l'idée de la preuve en Coq (aussi précise que possible) du lemme suivant :

   `Lemma not_A_A_1 : not (sys_g_1 A A 1).`

   Correction : La définition de $\neg A$ est $A \Rightarrow False$. D'après le lemme précédent si on a `sys_g_1 A A n` alors $n > 4$ donc on aurait $1 > 4$ d'où la contradiction.

```
Lemma not_1_ge_4 : not (1 >= 4).
Proof.
omega.
Qed.

Lemma not_A_A_1 : not (sys_g_1 A A 1).
Proof.
intro.
assert (1>=4).
apply sys_g_1_n_4 with (X:=A) (Y:=A).
assumption.
apply not_1_ge_4.
assumption.
Qed.
```

6. La définition inductive proposée ne convient pas. Que dire de `G(A,A,1)` ? Proposer une définition alternative `sys_g_2`.
   Correction :

```
Inductive sys_g_2 : joueur -> joueur -> nat -> Prop :=
| A4a : sys_g_2 A B 0
| A4b : sys_g_2 B A 0
| S1a : forall n, sys_g_2 A B n ->  sys_g_2 A A (n+1)
| S2a : forall n, sys_g_2 A B n ->  sys_g_2 A A (n+2)
| S3a : forall n, sys_g_2 A B n ->  sys_g_2 A A (n+3)
| S4a : forall n, sys_g_2 A B n ->  sys_g_2 A B (n+4)
| S1b : forall n, sys_g_2 B A n ->  sys_g_2 B B (n+1)
| S2b : forall n, sys_g_2 B A n ->  sys_g_2 B B (n+2)
| S3b : forall n, sys_g_2 B A n ->  sys_g_2 B B (n+3)
| S4b : forall n, sys_g_2 B A n ->  sys_g_2 B A (n+4)
.
```

7. Enoncer un lemme exprimant le fait que le prédicat `sys_g_1` est symétrique en A et B. Donner l'idée de la preuve en Coq (aussi précise que possible).
   On fait une preuve par induction en appliquant le contructeur symétrique dans chacun des cas.
   Correction :

```
Lemma sym : forall n, sys_g_2 A B n -> sys_g_2 B A n.
Proof.
intros.
induction H.
apply A4b;assumption.
apply A4a;assumption.
apply S1a;assumption.
apply S2a;assumption.
apply S3a;assumption.
apply S4b;assumption.
apply S1b;assumption.
apply S2b;assumption.
apply S3b;assumption.
apply S4a;assumption.
Qed.
```

or_introl	$\forall A\ B : Prop, A \to A \vee B$
or_intror	$\forall A\ B : Prop, B \to A \vee B$
or_ind	$\forall A\ B\ P : Prop, (A \to P) \to (B \to P) \to A \vee B \to P$
conj	$\forall A\ B : Prop, A \to B \to A \wedge B$
and_ind	$\forall A\ B\ P : Prop, (A \to B \to P) \to A \wedge B \to P$

DÉDUCTION NATURELLE

$$\frac{}{\Gamma \vdash A}\ \text{si } A \in \Gamma \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ \text{Intro} \Rightarrow \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \text{Elim} \Rightarrow$$

FIGURE 1 – Déduction naturelle : logique minimale

$$\frac{}{\Gamma \vdash A}\ \text{si } A \in \Gamma \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ \text{Intro} \Rightarrow \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \text{Elim} \Rightarrow$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash P}\ \text{Elim } \bot$$

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \text{Intro } \neg \qquad \frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}\ \text{Elim } \neg$$

$$\frac{\Gamma \vdash P \qquad \Gamma \vdash Q}{\Gamma \vdash P \wedge Q}\ \text{Intro } \wedge \qquad \frac{\Gamma \vdash P \wedge Q}{\Gamma \vdash P}\ \text{Elim } \wedge\text{g} \qquad \frac{\Gamma \vdash P \wedge Q}{\Gamma \vdash Q}\ \text{Elim } \wedge\text{d}$$

$$\frac{\Gamma \vdash P}{\Gamma \vdash P \vee Q}\ \text{Intro } \vee\text{g} \qquad \frac{\Gamma \vdash Q}{\Gamma \vdash P \vee Q}\ \text{Intro } \vee\text{d}$$

$$\frac{\Gamma \vdash P \vee Q \qquad \Gamma, P \vdash R \qquad \Gamma, Q \vdash R}{\Gamma \vdash R}\ \text{Elim } \vee$$

FIGURE 2 – Déduction naturelle : logique intuitionniste

$$\frac{\Gamma, \neg P \vdash \bot}{\Gamma \vdash P}\ \text{RAA}$$

FIGURE 3 – Déduction naturelle : logique classique

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x\, A}\ \forall \text{ intro } (x \text{ n'est pas libre dans } \Gamma) \qquad \frac{\Gamma \vdash \forall x\, A}{\Gamma \vdash A[x \leftarrow t]}\ \forall \text{ elim}$$

$$\frac{\Gamma \vdash A[x \leftarrow t]}{\Gamma \vdash \exists x\, A}\ \exists \text{ intro} \qquad \frac{\Gamma \vdash \exists x\, A \qquad \Gamma, A \vdash B}{\Gamma \vdash B}\ \exists \text{ elim } (x \text{ n'est pas libre dans } \Gamma \text{ ni } B)$$

FIGURE 4 – Déduction naturelle : logique des prédicats