Université de Strasbourg
Ingénierie de la preuve   Feuille de CT

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 :

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

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

   (c) Donner le terme de preuve correspondant.

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

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

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

   (c) Donner le terme de preuve correspondant.

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 ?

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 demandèes sont celles qui s'appliquent lors de l'appel à la tactique `simpl`.
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.

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.
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.
3. Donner la preuve en Coq de fait que `sys_g_1 A A 5`.
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.
   ```
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).
   ```
6. La définition inductive proposée ne convient pas. Que dire de `G(A,A,1)` ? Proposer une définition alternative `sys_g_2`.
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.

`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