Spécifications formelles, vérification, validation (HMIN203)

Master AIGLE

Département Informatique

Faculté des Sciences de Montpellier

Examen du 17 mai 2016

Tous les documents sont autorisés. Les ordinateurs portables sont également autorisés, mais sans le réseau, et vous ne pouvez pas exécuter Coq.
L'examen dure 2h. Le barème est donné à titre indicatif. Le sujet comporte 2 pages et il y a 3 exercices.

Exercice 1 (7 pts)

1. Démontrer dans LK les propositions suivantes en logique du premier ordre :
   - $(\forall x.P(x) \Rightarrow Q(x)) \Rightarrow (\exists x.P(x)) \Rightarrow (\exists x.Q(x))$;
   - $\exists y.P(y) \Rightarrow \forall x.P(x)$
     (indice : utiliser la contraction droite et instancier y avec n'importe quel terme).
2. Dans la logique implicative minimale, nous rajoutons le connecteur « $\wedge$ » de la façon suivante :

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge_I$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge_{E1} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge_{E2}$$

   Dans le λ-calcul simplement typé, nous rajoutons les couples, ainsi que les projecteurs comme suit :
   - Si t_1 et t_2 sont des termes, alors (t_1, t_2) est un terme ;
   - Si t est un terme, alors $\mathrm{fst}\ t$ et $\mathrm{snd}\ t$ sont des termes.

   Nous étendons également les types avec le produit cartésien de la manière suivante :
   - Si τ_1 et τ_2 sont des types, alors $\tau_1 \times \tau_2$ est un type.

   Les règles de typage de ces nouveaux termes sont définies comme suit :

$$\frac{\Gamma \vdash t_1 : \tau_1 \quad \Gamma \vdash t_2 : \tau_2}{\Gamma \vdash (t_1, t_2) : \tau_1 \times \tau_2}\ \mathsf{Tup}$$

$$\frac{\Gamma \vdash t : \tau_1 \times \tau_2}{\Gamma \vdash \mathrm{fst}\ t : \tau_1}\ \mathsf{Fst} \qquad \frac{\Gamma \vdash t : \tau_1 \times \tau_2}{\Gamma \vdash \mathrm{snd}\ t : \tau_2}\ \mathsf{Snd}$$

Sachant que dans l'isomorphisme de Curry-Howard, nous souhaitons faire correspondre les règles de preuves $\wedge_I$, $\wedge_{E1}$, et $\wedge_{E2}$, aux règles de typage Tup, Fst, et Snd respectivement, répondre aux questions suivantes :

(a) Écrire les fonctions de correspondance Φ et φ pour ce nouveau connecteur (le « $\wedge$ ») et les nouvelles règles de preuve correspondantes ;

(b) Donner les λ-termes correspondants aux preuves de $A \Rightarrow B \Rightarrow A \wedge B$ et $A \wedge B \Rightarrow A$.

Exercice 2 (7 pts)

Dans ce qui suit, vous pouvez utiliser soit une notation mathématique (en logique du premier ordre), soit du code Coq (sauf pour la partie preuve, qui devra être faite semi-formellement en logique du premier ordre).

1. Spécifier inductivement le comportement de la suite de Fibonacci ;
2. Écrire la suite de Fibonacci comme une fonction ;
3. Écrire le schéma d'induction fonctionnelle correspondant à la fonction précédemment écrite ;
4. Démontrer en utilisant ce schéma que la fonction est conforme à sa spécification.

On rappelle la définition de la suite de Fibonacci :

$$u_n = \begin{cases} 0, \text{ si } n = 0 \\ 1, \text{ si } n = 1 \\ u_{n-1} + u_{n-2}, \text{ sinon} \end{cases}$$

Exercice 3 (7 pts)

En utilisant la logique de Hoare, démontrer la validité du triplet suivant (ce qui revient à démontrer que le programme ci-dessous implante la fonction factorielle) :

$\{\}$
$i := 0;$
$r := 1;$
while i != n do
  $i := i + 1;$
  $r := r \times i;$
$\{r = n!\}$