Vérification (HAI603I)

Licence Informatique
Département Informatique
Faculté des Sciences de Montpellier
Université de Montpellier

Examen du 30 juin 2022

Aucun document n'est autorisé. L'examen dure 2h. Le barème est donné à titre indicatif. Le sujet comporte 1 page et il y a 3 exercices.

Exercice 1 (7 pts)

Démontrer dans le système $\text{LJ}_{\textsf{EQ}}$ les séquents suivants :

1. $\vdash (\forall x.P(x) \Rightarrow Q(x)) \Rightarrow P(a) \Rightarrow \exists x.Q(x)$
2. $\forall x.x + 0 \doteq x, \forall x, y.x + y \doteq y + x \vdash \forall x.0 + (x + 0) \doteq x$

où P et Q sont des symboles de prédicat d'arité 1, « $+$ » un symbole de fonction d'arité 2, et a et 0 des constantes.

Exercice 2 (8 pts)

Dans ce qui suit, vous pouvez utiliser soit une notation mathématique (en logique du premier ordre), soit du code Coq (sauf pour les parties preuves, qui devront être faites semi-formellement en logique du premier ordre).

1. Écrire une relation inductive *even_decr_list* qui détermine si une liste d'entiers naturels est une liste d'entiers pairs décroissante de deux en deux jusqu'à 0. Par exemple, on a *even_decr_list*([0]) et *even_decr_list*([4; 2; 0]), mais pas *even_decr_list*([4; 0]).
2. Démontrer que : *even_decr_list*([4; 2; 0]).
3. Écrire la fonction f_{edl} qui teste si une liste d'entiers naturels est une liste d'entiers pairs décroissante jusqu'à 0. Par exemple, $f_{edl}([4;2;0])$ retourne vrai mais $f_{edl}([4;2;1])$ retourne faux.
4. Écrire le schéma d'induction fonctionnelle associé à la fonction f_{edl}.
5. Énoncer les théorèmes de correction et complétude de la fonction f_{edl} vis-à-vis de la spécification *even_decr_list* (on souhaite juste les énoncés, pas les preuves).

Exercice 3 (5 pts)

En utilisant les règles de la logique de Hoare (les règles sont données à la fin de l'exercice), démontrer la validité des triplets suivants :

1. $\{x = 1 \wedge y = 2\}\ t := x; x := y; y := t\ \{x = 2 \wedge y = 1\}$
2. $\{x \geq 0\}$ if x != 0 then $x := x - 1$ else $x := x + 1$ $\{x \geq 0\}$

Règles de la logique de Hoare

$$\frac{}{\{P\}\ \text{skip}\ \{P\}}\ \text{skip} \qquad\qquad \frac{}{\{P(e)\}\ x := e\ \{P(x)\}}\ :=$$

$$\frac{\{P\}\ i_1\ \{Q\} \qquad \{Q\}\ i_2\ \{R\}}{\{P\}\ i_1; i_2\ \{R\}}\ ;$$

$$\frac{\{P \wedge e\}\ i_1\ \{Q\} \qquad \{P \wedge \neg e\}\ i_2\ \{Q\}}{\{P\}\ \text{if}\ e\ \text{then}\ i_1\ \text{else}\ i_2\ \{Q\}}\ \text{if}$$

$$\frac{\{I \wedge e\}\ i\ \{I\}}{\{I\}\ \text{while}\ e\ \text{do}\ i\ \{I \wedge \neg e\}}\ \text{while}$$

$$\frac{\{P'\}\ i\ \{Q'\} \qquad P \Rightarrow P' \qquad Q' \Rightarrow Q}{\{P\}\ i\ \{Q\}}\ \text{Aff}$$

Règles du système $\mathrm{LJ}_{\mathsf{EQ}}$

$$\frac{}{\Gamma, A \vdash A}\ \mathsf{ax} \qquad\qquad \frac{\Gamma \vdash A \qquad \Gamma, A \vdash B}{\Gamma \vdash B}\ \mathsf{cut}$$

$$\frac{\Gamma, A, A \vdash B}{\Gamma, A \vdash B}\ \mathsf{cont}$$

$$\frac{\Gamma \vdash A \qquad \Gamma, B \vdash C}{\Gamma, A \Rightarrow B \vdash C}\ \Rightarrow_{\mathsf{left}} \qquad\qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ \Rightarrow_{\mathsf{right}}$$

$$\frac{\Gamma \vdash A \qquad \Gamma, B \vdash C}{\Gamma, A \Leftrightarrow B \vdash C}\ \Leftrightarrow_{\mathsf{left1}}$$

$$\frac{\Gamma \vdash B \qquad \Gamma, A \vdash C}{\Gamma, A \Leftrightarrow B \vdash C}\ \Leftrightarrow_{\mathsf{left2}} \qquad\qquad \frac{\Gamma, A \vdash B \qquad \Gamma, B \vdash A}{\Gamma \vdash A \Leftrightarrow B}\ \Leftrightarrow_{\mathsf{right}}$$

$$\frac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge_{\mathsf{left}} \qquad\qquad \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge_{\mathsf{right}}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee_{\mathsf{right1}}$$

$$\frac{\Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}\ \vee_{\mathsf{left}} \qquad\qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee_{\mathsf{right2}}$$

$$\frac{\Gamma \vdash A}{\Gamma, \neg A \vdash B}\ \neg_{\mathsf{left}} \qquad\qquad \frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg_{\mathsf{right}}$$

$$\frac{}{\Gamma, \bot \vdash A}\ \bot_{\mathsf{left}} \qquad\qquad \frac{}{\Gamma \vdash \top}\ \top_{\mathsf{right}}$$

$$\frac{\Gamma, A(t) \vdash B}{\Gamma, \forall x.A(x) \vdash B}\ \forall_{\mathsf{left}} \qquad\qquad \frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x.A(x)}\ \forall_{\mathsf{right}},\ x \notin \Gamma$$

$$\frac{\Gamma, A(x) \vdash B}{\Gamma, \exists x.A(x) \vdash B}\ \exists_{\mathsf{left}},\ x \notin \Gamma, B \qquad\qquad \frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x.A(x)}\ \exists_{\mathsf{right}}$$

$$\frac{}{\Gamma \vdash s \doteq s}\ \mathsf{refl}$$

$$\frac{\Gamma \vdash P(s) \qquad \forall \vec{x}.s' \doteq t' \in \Gamma \qquad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash P(t)}\ =_{\mathsf{right1}}$$

$$\frac{\Gamma \vdash P(t) \qquad \forall \vec{x}.s' \doteq t' \in \Gamma \qquad s = \sigma(s'), t = \sigma(t')}{\Gamma \vdash P(s)}\ =_{\mathsf{right2}}$$

$$\frac{\Gamma, P(s) \vdash A \qquad \forall \vec{x}.s' \doteq t' \in \Gamma \qquad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(t) \vdash A}\ =_{\mathsf{left1}}$$

$$\frac{\Gamma, P(t) \vdash A \qquad \forall \vec{x}.s' \doteq t' \in \Gamma \qquad s = \sigma(s'), t = \sigma(t')}{\Gamma, P(s) \vdash A}\ =_{\mathsf{left2}}$$