Modélisation et Programmation – Sessions 1 et 3 – 6/11/2018

Prénom : Nom : Groupe :

Les exercices sont indépendants les uns des autres. Lisez le sujet avant de commencer. Traitez les exercices dans votre ordre de préférence.
Dans tous les exercices, vous veillerez à justifier vos résultats, par exemple en faisant apparaître le nom des règles utilisées, il en sera tenu compte dans la notation.
Les preuves demandées ont toutes été réalisées avec Coq et Why3 pour réduire les risques d'erreurs. Si vous pensez avoir trouvé une erreur, indiquez le sur votre copie, corrigez la et poursuivez votre composition.

Exercice 1 Modéliser en logique des prédicats, sous la forme de formules bien formées, l'énoncé suivant : « Tous les étudiants inscrits dans le département Sciences du Numérique étudient l'Informatique, mais seulement certains d'entre eux choisirons de travailler dans ce domaine. »

Exercice 2 Soient A et B des variables propositionnelles, montrer, **en utilisant les propriétés des opérateurs de logique des propositions** rappelées en annexe A, que la formule suivante est une tautologie :

$$((A \to C) \land (B \to C)) \to ((A \lor B) \to C)$$

Exercice 3 Soient A et B des variables propositionnelles, montrer, **en utilisant la déduction naturelle constructive (c'est-à-dire sans les règles du tiers-exclu (TE dans le résumé de cours) et de l'absurde classique (A dans le résumé de cours))**, que la formule suivante est une tautologie :

$$(\neg(A \vee B)) \rightarrow ((\neg A) \wedge (\neg B))$$

Exercice 4 Soient A et B des variables propositionnelles, montrer, **en utilisant la déduction naturelle classique (y compris les règles du tiers-exclu ou de l'absurde classique)**, que la formule suivante est une tautologie :

$$(\neg(A \wedge B)) \rightarrow ((\neg A) \vee (\neg B))$$

Exercice 5 Prouver la correction totale du triplet de Hoare suivant pour un programme calculant le produit de deux entiers positifs $\mathtt{A}$ et $\mathtt{B}$. Nous vous suggérons d'exploiter $\mathtt{R} = \mathtt{A} \times (\mathtt{B} - \mathtt{I})$ comme invariant et $\mathtt{I}$ comme variant. Vous compléterez l'invariant si nécessaire pour construire la preuve. Vous détaillerez sur la page suivante la preuve des obligations obtenues.

$\{\mathtt{A} \geq 0 \wedge \mathtt{B} \geq 0\}$

```
R := 0;

I := B

while (0 < I) do

        R := R + A;

        I := I - 1

od;
```

$\{\mathtt{R} = \mathtt{A} \times \mathtt{B}\}$

Exercice 6 Nous considérons la spécification des listes munie des équations étudiées en cours et travaux dirigés :

(a) $\forall l \in \texttt{liste}(A).\ \texttt{append}(\texttt{Nil}, l) = l$
(b) $\forall t \in A. \forall l, q \in \texttt{liste}(A).\ \texttt{append}(\texttt{Cons}(t,\ q), l) = \texttt{Cons}(t,\ \texttt{append}(q, l))$
(c) $\forall l \in \texttt{liste}(A).\ \texttt{append}(l, \texttt{Nil}) = l$
(d) $\forall l_1, l_2, l_3 \in \texttt{liste}(A).\ \texttt{append}(l_1, \texttt{append}(l_2, l_3)) = \texttt{append}(\texttt{append}(l_1, l_2), l_3)$

Nous complétons cette spécification par la fonction $\texttt{snoc}(l,\ e)$ qui ajoute l'élément e à la fin de la liste l.
Le comportement de cette fonction peut être modélisé par les équations suivantes :

(e) $\forall e \in A.\ \texttt{snoc}(\texttt{Nil},\ e) = \texttt{Cons}(e,\ \texttt{Nil})$
(f) $\forall e \in A. \forall t \in A. \forall q \in \texttt{liste}(A).\ \texttt{snoc}(\texttt{Cons}(t,\ q),\ e) = \texttt{Cons}(t,\ \texttt{snoc}(q,\ e))$

En utilisant ces équations comme des axiomes et en introduisant si nécessaire des lemmes intermédiaires, montrer que ces opérations vérifient la propriété suivante :

(g) $\forall e \in A. \forall l \in \texttt{liste}(A).\ \texttt{snoc}(l,\ e) = \texttt{append}(l, \texttt{Cons}(e,\ \texttt{Nil}))$

(h) $\forall e \in A. \forall l_1 \in \texttt{liste}(A). \forall l_2 \in \texttt{liste}(A).\ \ \texttt{snoc}(\texttt{append}(l_1, l_2),\ e) = \texttt{append}(l_1, \texttt{snoc}(l_2,\ e))$

Exercice 7 Un nombre décimal non nul normalisé est composé d'une mantisse suivie d'un exposant optionnel.
La mantisse ne contient pas de partie entière. Elle débute par un signe optionnel, `+` (plus) ou `-` (moins), suivi par le chiffre `0` (zéro) puis par le caractère `.` (point) puis par un chiffre différent de zéro et enfin par une suite de chiffres éventuellement vide.
Un exposant débute par la lettre `e` en minuscule ou majuscule, suivie par un signe optionnel `+` (plus) ou `-` (moins), puis par un chiffre différent de zéro et enfin par une suite de chiffre éventuellement vide.

1. Proposer une expression régulière qui modélise le langage des nombres décimaux normalisés.

Exercice 8 Soit la grammaire qui modélise la partie droite de l'initialisation explicite de tableaux d'entiers en langage C, C++, C#, JAVA, ..., $G_0 = (A, V, T, P)$ composée des non-terminaux $V = \{L\ E\ T\}$, de l'axiome T, des terminaux $A = \{\texttt{entier}\ ,\ \{\ \}\}$ et de l'ensemble P de règles suivantes :

1. $T \rightarrow \{\ L\ \}$
2. $L \rightarrow L\ ,\ E$
3. $L \rightarrow E$
4. $E \rightarrow \texttt{entier}$
5. $E \rightarrow T$

Voici un exemple de mots modélisés par cette grammaire :

```
{ 1, { 2 }, 3 }
```

1. Construire la dérivation la plus à gauche de cet exemple selon cette grammaire ;

2. Donner l'arbre de dérivation de cet exemple selon cette grammaire ;

3. Peut on modéliser ce langage par une expression régulière ? Pourquoi ?

4. Donner une grammaire au format graphique de Conway modélisant ce langage.

5. Donner une grammaire au format EBNF modélisant ce langage.

A Logique des propositions : Vision sémantique

A.1 Tables de vérité

La sémantique de $\top$ (respectivement $\bot$) est représenté par V (respectivement F).

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \to B$	$A \leftrightarrow B$
F	F	V	F	F	V	V
F	V	V	F	V	V	F
V	F	F	F	V	F	F
V	V	F	V	V	V	V

A.2 Relation d'équivalence sémantique des formules bien formées

$\varphi = \psi$ si et seulement si les deux formules bien formées φ et ψ ont la même table de vérité.

	$A \to B = \neg A \vee B$ $A \leftrightarrow B = (A \to B) \ \wedge \ (B \to A)$
Idempotence	$A \wedge A = A$ $A \vee A = A$
	$A \wedge \neg A = \bot$ $A \vee \neg A = \top$ $A \wedge \bot = \bot$ $A \wedge \top = A$ $A \vee \bot = A$ $A \vee \top = \top$ $\neg\neg A = A$
Commutativité	$A \wedge B = B \wedge A$ $A \vee B = B \vee A$
Associativité	$(A \wedge B) \wedge C = A \wedge (B \wedge C)$ $(A \vee B) \vee C = A \vee (B \vee C)$
Distributivité	$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$ $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$
De Morgan	$\neg(A \wedge B) = \neg A \vee \neg B$ $\neg(A \vee B) = \neg A \wedge \neg B$
Simplification	$A \vee (\neg A \wedge B) = A \vee B$ $A \wedge (\neg A \vee B) = A \wedge B$ $A \vee (A \wedge B) = A$ $A \wedge (A \vee B) = A$

B Logique des propositions : Vision syntaxique

B.1 Déduction naturelle constructive

Hypothèse	$\dfrac{}{\Gamma,\, \varphi \vdash \varphi}\ Hyp(\Gamma; \varphi)$	
Opérateur	Introduction	Elimination
$\rightarrow$	$\dfrac{\Gamma,\, \varphi \vdash \psi}{\Gamma \vdash \varphi \rightarrow \psi}\ I_{\rightarrow}(\Gamma; \varphi; \psi)$	$\dfrac{\Gamma \vdash \varphi \rightarrow \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}\ E_{\rightarrow}(\Gamma; \varphi; \psi)$
$\wedge$	$\dfrac{\Gamma \vdash \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}\ I_{\wedge}(\Gamma; \varphi; \psi)$	$\dfrac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi}\ E^G_{\wedge}(\Gamma; \varphi; \psi)$ $\dfrac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}\ E^D_{\wedge}(\Gamma; \varphi; \psi)$
$\vee$	$\dfrac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}\ I^G_{\vee}(\Gamma; \varphi; \psi)$ $\dfrac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}\ I^D_{\vee}(\Gamma; \varphi; \psi)$	$\dfrac{\Gamma \vdash \varphi \vee \psi \quad \Gamma,\, \varphi \vdash \chi \quad \Gamma,\, \psi \vdash \chi}{\Gamma \vdash \chi}\ E_{\vee}(\Gamma; \varphi; \psi; \chi)$
$\neg$	$\dfrac{\Gamma,\, \varphi \vdash \bot}{\Gamma \vdash \neg\varphi}\ I_{\neg}(\Gamma; \varphi)$	$\dfrac{\Gamma \vdash \varphi \quad \Gamma \vdash \neg\varphi}{\Gamma \vdash \bot}\ E_{\neg}(\Gamma; \varphi)$
$\bot$	$\dfrac{\Gamma \vdash \varphi \quad \Gamma \vdash \neg\varphi}{\Gamma \vdash \bot}\ I_{\bot}(\Gamma; \varphi)$	$\dfrac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}\ E_{\bot}(\Gamma; \varphi)$

B.2 Déduction naturelle classique

Tiers-exclu	Preuve par l'absurde
$\dfrac{}{\Gamma \vdash \varphi \vee \neg\varphi}\ TE(\Gamma; \varphi)$	$\dfrac{\Gamma,\, \neg\varphi \vdash \bot}{\Gamma \vdash \varphi}\ Abs(\Gamma, \varphi)$

C Logique des prédicats : Vision sémantique

C.1 Relation d'équivalence sémantique des formules bien formées

$\varphi = \psi$ si et seulement si les deux formules bien formées φ et ψ ont la même sémantique, c'est à dire sont valides sémantiquement pour les mêmes modèles $(\forall \mathcal{M}, (\mathcal{M} \models \varphi) \leftrightarrow (\mathcal{M} \models \psi))$.

$\mathcal{U} \neq \emptyset$	$\forall x.\ \varphi = \bigwedge_{x \in \mathcal{U}} \varphi$	$\exists x.\ \varphi = \bigvee_{x \in \mathcal{U}} \varphi$
$\mathcal{U} = \emptyset$	$\forall x.\ \varphi = \top$	$\exists x.\ \varphi = \bot$

$$
\begin{array}{rl}
\forall x.\ \varphi = \varphi & x \notin VL(\varphi) \wedge \mathcal{U} \neq \emptyset \\
\exists x.\ \varphi = \varphi & x \notin VL(\varphi) \wedge \mathcal{U} \neq \emptyset \\
\forall x.\ \varphi = \forall y.\ [y/x]\,\varphi & y \text{ inutilisée} \\
\exists x.\ \varphi = \exists y.\ [y/x]\,\varphi & y \text{ inutilisée} \\
\forall x.\ (\forall y.\ \varphi) = \forall y.\ (\forall x.\ \varphi) & \\
\exists x.\ (\exists y.\ \varphi) = \exists y.\ (\exists x.\ \varphi) & \\
\neg(\forall x.\ \varphi) = \exists x.\ (\neg\varphi) & \\
\neg(\exists x.\ \varphi) = \forall x.\ (\neg\varphi) & \\
\forall x.\ (\varphi \rightarrow \psi) = (\exists x.\ \varphi) \rightarrow \psi & x \notin VL(\psi) \\
\forall x.\ (\varphi \rightarrow \psi) = \varphi \rightarrow (\forall x.\ \psi) & x \notin VL(\varphi) \\
\exists x.\ (\varphi \rightarrow \psi) = (\forall x.\ \varphi) \rightarrow \psi & x \notin VL(\psi) \wedge \mathcal{U} \neq \emptyset \\
\exists x.\ (\varphi \rightarrow \psi) = \varphi \rightarrow (\exists x.\ \psi) & x \notin VL(\varphi) \wedge \mathcal{U} \neq \emptyset \\
\forall x.\ (\varphi \wedge \psi) = (\forall x.\ \varphi) \wedge (\forall x.\ \psi) & \\
\forall x.\ (\varphi \vee \psi) = (\forall x.\ \varphi) \vee \psi & x \notin VL(\psi) \\
\exists x.\ (\varphi \vee \psi) = (\exists x.\ \varphi) \vee (\exists x.\ \psi) & \\
\exists x.\ (\varphi \wedge \psi) = (\exists x.\ \varphi) \wedge \psi & x \notin VL(\psi)
\end{array}
$$

D Logique des prédicats : Vision syntaxique

D.1 Déduction naturelle constructive

Opérateur	Introduction	Elimination
$\forall.$	$\dfrac{\Gamma \vdash \varphi}{\Gamma \vdash \forall x.\ \varphi}\ I_\forall(\Gamma; x; \varphi)\ (x \notin VL(\Gamma))$	$\dfrac{\Gamma \vdash \forall x.\ \varphi}{\Gamma \vdash [t/x]\,\varphi}\ E_\forall(\Gamma; x; \varphi; t)$
$\exists.$	$\dfrac{\Gamma \vdash [t/x]\,\varphi}{\Gamma \vdash \exists x.\ \varphi}\ I_\exists(\Gamma; x; \varphi)$	$\dfrac{\Gamma \vdash \exists x.\ \varphi}{\Gamma \vdash [f(\vec{x})/x]\,\varphi}\ E_\exists^{SK}(\Gamma; x; \varphi)\ (\vec{x} = VL(\Gamma) \cup VL(\exists x.\ \varphi))$ $\dfrac{\Gamma \vdash \exists x.\ \varphi \qquad \Gamma,\ \varphi \vdash \psi}{\Gamma \vdash \psi}\ E_\exists^{MP}(\Gamma; x; \varphi)\ (x \notin VL(\Gamma) \cup VL(\psi))$

E Logique de Floyd/Hoare

$$\dfrac{}{\{\psi\}\ \text{skip}\ \{\psi\}}\ \text{skip} \qquad \dfrac{}{\{[E/x]\,\psi\}\ x := E\ \{\psi\}}\ \text{assign}$$

$$\dfrac{\{\varphi\}\ P\ \{\chi\} \qquad \{\chi\}\ Q\ \{\psi\}}{\{\varphi\}\ P\ ;Q\ \{\psi\}}\ \text{sequence}$$

$$\dfrac{\{\varphi \wedge C\}\ P\ \{\psi\} \qquad \{\varphi \wedge \neg C\}\ Q\ \{\psi\}}{\{\varphi\}\ \text{if } C \text{ then } P \text{ else } Q \text{ fi}\ \{\psi\}}\ \text{conditional}$$

$$\dfrac{\{\varphi \wedge C\}\ P\ \{\varphi\}}{\{\varphi\}\ \text{while } C \text{ invariant } \varphi \text{ do } P \text{ od}\ \{\varphi \wedge \neg C\}}\ \text{partial loop}$$

$$\dfrac{\{\varphi \wedge C \wedge E \in \mathbb{N} \wedge V = E\}\ P\ \{\varphi \wedge E \in \mathbb{N} \wedge V > E\}}{\{\varphi \wedge E \in \mathbb{N}\}\ \text{while } C \text{ invariant } \varphi \text{ variant } E \text{ do } P \text{ od}\ \{\varphi \wedge \neg C\}}\ \text{total loop}$$

$$\dfrac{\varphi \to \chi \qquad \{\chi\}\ P\ \{\psi\}}{\{\varphi\}\ P\ \{\psi\}}\ \text{weaken} \qquad \dfrac{\{\varphi\}\ P\ \{\chi\} \qquad \chi \to \psi}{\{\varphi\}\ P\ \{\psi\}}\ \text{strengthen}$$

F Expressions régulières : Equivalence sémantique

L'opérateur de concaténation/juxtaposition . est implicite pour ne pas surcharger l'écriture des expressions : $e_1.e_2$ est notée $e_1\,e_2$.

$$\begin{array}{ll}
\emptyset\, e = e\, \emptyset = \emptyset & \Lambda\, e = e\, \Lambda = e \\
e \mid \emptyset = \emptyset \mid e = e & e \mid e = e \\
e_1\,(e_2\,e_3) = (e_1\,e_2)\,e_3 & e_1 \mid (e_2 \mid e_3) = (e_1 \mid e_2) \mid e_3 \\
e_1\,(e_2 \mid e_3) = (e_1\,e_2) \mid (e_1\,e_3) & (e_1 \mid e_2)\,e_3 = (e_1\,e_2) \mid (e_1\,e_3) \\
e_1 \mid e_2 = e_2 \mid e_1 & \emptyset^\star = \Lambda^\star = \Lambda \\
e^\star = \Lambda \mid e^+ & e^+ = e\,e^\star = e^\star\,e \\
e^\star\,e^\star = e^\star & e^{\star\star} = e^\star \\
e = e^\star \Leftrightarrow e = e\,e \wedge e \neq \emptyset & e\,e^\star = e^\star \Leftrightarrow \Lambda \in L(e) \\
(e_1^\star\,e_2^\star)^\star = (e_1 \mid e_2)^\star = (e_1^\star \mid e_2^\star)^\star & \\
(e_1^\star\,e_2)^\star\,(e_1^\star) = (e_1 \mid e_2)^\star = e_1^\star\,(e_2\,(e_1^\star))^\star &
\end{array}$$