Master 1 InformatiqueAnnée 2010/2011

SORBONNE UNIVERSITÉS

Logique pour l'Informatique Avancée
MI067 STL
Décembre 2010

Examen réparti n° 2

Vous traiterez les exercices dans l'ordre que vous souhaitez. La durée de cet examen est de 2 heures. Vous pouvez utiliser vos notes de cours et celles mises en ligne par vos enseignants.

Exercice I : *Quelques propositions*

Voici 6 propositions :

1. $(P \to P) \to Q$
2. $(P \to Q) \to P$
3. $(Q \to P) \to P$
4. $P \to (P \to Q)$
5. $P \to (Q \to P)$
6. $Q \to (P \to P)$

Parmi elles, certaines sont des tautologies, d'autres non.

Question (I.1) Pour chacune de ces propositions :

1. si ce n'est pas une tautologie, donnez une interprétation $\mathcal{I}$ de P et Q qui la rende fausse.
2. sinon, montrez que c'est une tautologie. Vous pourrez utiliser la méthode de votre choix.

Réponses

1. $(P \to P) \to Q$ n'est pas une tautologie.
   Si $\mathcal{I}(Q) = \bot$ alors $\mathcal{I}((P \to P) \to Q) = \bot$ quelque soit la valeur de $\mathcal{I}(P)$.
2. $(P \to Q) \to P$ n'est une tautologie.
   Si $\mathcal{I}(P) = \mathcal{I}(Q) = \bot$ alors $\mathcal{I}(P \to Q) = \top$ et $\mathcal{I}((P \to Q) \to P) = \bot$.

3. $(Q \to P) \to P$ n'est pas une tautologie.
   Si $\mathcal{I}(P) = \mathcal{I}(Q) = \bot$ alors $\mathcal{I}(Q \to P) = \top$ et $\mathcal{I}((Q \to P) \to P) = \bot$.
4. $P \to (P \to Q)$ n'est pas une tautologie.
   Si $\mathcal{I}(P) = \top$ et $\mathcal{I}(Q) = \bot$ alors $\mathcal{I}(P \to Q) = \bot$ et $\mathcal{I}(P \to (P \to Q)) = \bot$.
5. $P \to (Q \to P)$ est une tautologie. Par la méthode des tables de vérité :

P	Q	$Q \to P$	$P \to (Q \to P)$
$\top$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\top$	$\top$
$\bot$	$\top$	$\top$	$\top$
$\bot$	$\bot$	$\top$	$\top$

6. $Q \to (P \to P)$ est une tautologie.
   Quelle que soit la valeur de $\mathcal{I}(P)$, on a tooujours $\mathcal{I}(P \to P) = \top$ (c'est-à-dire que $P \to P$ est une tautologie. Donc
   – si $\mathcal{I}(Q) = \top$ alors $\mathcal{I}(Q \to (P \to P)) = \top$;
   – et si $\mathcal{I}(Q) = \bot$ alors $\mathcal{I}(Q \to (P \to P)) = \top$.

Exercice II : *Satisfaisabilité et conséquence sémantique*

Question (II.1) Montrez que si $\mathcal{M}, \rho \models F \to G$ et $\mathcal{M}, \rho \models F$ alors $\mathcal{M}, \rho \models G$.
C'est la régle du modus ponens au niveau sémantique. Il faut utiliser la définition de $\models$.

Réponses

Raisonnons par l'absurde. C'est-à-dire supposons que
H1 $\mathcal{M}, \rho \models F \to G$, c'est-à-dire $\mathcal{I}^M(F \to G)_\rho = \top$ et
H2 $\mathcal{M}, \rho \models F$, c'est-à-dire $\mathcal{I}^M(F)_\rho = \top$ et
H3 $\mathcal{M}, \rho \not\models G$, c'est-à-dire $\mathcal{I}^M(G)_\rho = \bot$ que nous cherchons à contredire.
Par définition de $\mathcal{I}$ et de l'hypothèse H1, on déduit que

1. $\mathcal{I}^M(F)_\rho = \bot$ ou
2. $\mathcal{I}^M(F)_\rho = \mathcal{I}^M(G)_\rho = \top$

On ne peut avoir que $\mathcal{I}^M(F)_\rho = \bot$ car cela contredit l'hypothèse H2. On a donc $\mathcal{I}^M(F)_\rho = \mathcal{I}^M(G)_\rho = \top$, en particulier, $\mathcal{I}^M(G)_\rho = \top$, ce qui contredit l'hypothèse H3 ; ce qu'il fallait démontrer

---

Question (II.2) Soit l'ensemble d'hypothèses
$\Gamma = \{\forall x.(P(x) \to R(x)); \forall x.(Q(x) \to R(x)); \exists x.(Q(x) \vee P(x))\}$. Montrez que $\Gamma \models \exists x.R(x)$.
Vous pouvez utiliser le résultat de la question précédente pour raisonner.

Réponses

Informellement, le raisonnement est le suivant : de l'hypothèse $\exists x.(Q(x) \vee P(x))$ on déduit qu'il existe $m_0 \in \mathcal{M}$ tel que $Q(m_0) \vee P(m_0)$; des deux hypothèses $\forall x.(P(x) \to R(x))$ et $\forall x.(Q(x) \to R(x))$ on déduit qu'*en particulier* $P(m_0) \to R(m_0)$ et $Q(m_0) \to R(m_0)$. On utilise la disjonction $Q(m_0) \vee P(m_0)$ pour raisonner par cas :

– si $Q(m_0)$ alors, d'après le résultat ci-dessus et $Q(m_0) \to R(m_0)$ on a $R(m_0)$;
– si $P(m_0)$ alors, d'après le résultat ci-dessus et $P(m_0) \to R(m_0)$ on a $R(m_0)$;

Donc dans tous les cas, on a $R(m_0)$.

Plus formellement, pour montrer que $\Gamma \models \exists x.R(x)$, il faut montrer que pour tout $\mathcal{M}$ et tout ρ, si $\mathcal{M}, \rho \models \forall x.(P(x) \to R(x))$, si $\mathcal{M}, \rho \models \forall x.(Q(x) \to R(x))$ et si $\exists x.(Q(x) \vee P(x))$ alors $\mathcal{M}, \rho \models \exists x.R(x)$. On reprend alors les grandes lignes du raisonnment informel et on utilise les équivalence des FAITS (5) du cours :

– si $\exists x.(Q(x) \vee P(x))$, alors par 5.6, il existe $m_0 \in M$ (ensemble de base de $\mathcal{M}$) tel que $\mathcal{M}, \rho[x \mapsto m_0] \models Q(z) \vee P(z)$;
– si $\mathcal{M}, \rho \models \forall x.(P(x) \to R(x))$, alors, par 5.5, pour tout $m \in M$, $\mathcal{M}, \rho[x \mapsto m] \models P(x) \to R(x)$. Donc, en particulier, $\mathcal{M}, \rho[x \mapsto m_0] \models P(x) \to R(x)$;
– si $\mathcal{M}, \rho \models \forall x.(Q(x) \to R(x))$, alors, par 5.5, pour tout $m \in M$, $\mathcal{M}, \rho[y \mapsto m] \models Q(x) \to R(x)$. Donc, en particulier, $\mathcal{M}, \rho[x \mapsto m_0] \models Q(x) \to R(x)$;
– puisque $\mathcal{M}, \rho[x \mapsto m_0] \models Q(x) \vee P(x)$, par 5.2, on a que $\mathcal{M}, \rho[x \mapsto m_0] \models Q(x)$ ou $\mathcal{M}, \rho[x \mapsto m_0] \models P(x)$;
– on raisonne alors par cas :
  – si $\mathcal{M}, \rho[x \mapsto m_0] \models Q(x)$, par le résultat ci-dessus et $\mathcal{M}, \rho[x \mapsto m_0] \models Q(x) \to R(x)$, on a que $\mathcal{M}, \rho[x \mapsto m_0] \models R(x)$;
  – si $\mathcal{M}, \rho[x \mapsto m_0] \models P(x)$, par le résultat ci-dessus et $\mathcal{M}, \rho[x \mapsto m_0] \models P(x) \to R(x)$, on a que $\mathcal{M}, \rho[x \mapsto m_0] \models R(x)$;

  Dans tous les cas, on a qu'il existe $m_0 \in M$ tel que $\mathcal{M}, \rho[x \mapsto m_0] \models R(x)$, et donc, par 5.6, $\mathcal{M}, \rho \models \exists x.Q(x)$.

Question (II.3) Montrez que si $\mathcal{M}, \rho \models F \vee G$ et $\mathcal{M}, \rho \models \neg F$ alors $\mathcal{M}, \rho \models G$.
Vous pourrez utiliser un raisonnement par l'absurde. Il faut ici aussi revenir à la définition de $\models$.

Réponses

Par l'absurde : on suppose
– $\mathcal{M}, \rho \models F \vee G$, c'est-à-dire $\mathcal{I}^{\mathcal{M}}(F \vee G)_\rho = \top$ (c'est ce que l'on va chercher à contredire) et
– $\mathcal{M}, \rho \models \neg F$, c'est-à-dire $\mathcal{I}^{\mathcal{M}}(\neg F)_\rho = \top$ et
– $\mathcal{M}, \rho \not\models G$, c'est-à-dire $\mathcal{I}^{\mathcal{M}}(G)_\rho = \bot$.

De $\mathcal{I}^{\mathcal{M}}(\neg F)_\rho = \top$, on déduit, par définition de $\mathcal{I}$ que $\mathcal{I}^{\mathcal{M}}(F)_\rho = \bot$; on a donc que $\mathcal{I}^{\mathcal{M}}(F)_\rho = \mathcal{I}^{\mathcal{M}}(G)_\rho = \bot$; on en déduit, par définition de $\mathcal{I}$ que $\mathcal{I}^{\mathcal{M}}(F \vee G)_\rho = \bot$, ce qui contredit l'hypothèse $\mathcal{I}^{\mathcal{M}}(F \vee G)_\rho = \top$.

Question (II.4) Soit l'ensemble d'hypothèses
$\Gamma = \{\exists x.(P(x) \to R(x)); \forall x.(Q(x) \to R(x)); \forall x.(Q(x) \vee P(x))\}$. Montrez que $\Gamma \models \exists x.R(x)$.
Vous pourrez utiliser le résultat de la question précédente et de la première question de cet exercice. Un conseil : utilisez d'abord l'hypothèse $\exists x.(P(x) \to R(x))$.

Exercice III : *Déduction naturelle*

Question (III.1) Donnez une preuve en déduction naturelle des séquents suivants :

1. $((F \to G) \to H); (F \wedge G) \vdash H$
2. $(F \to G); \neg G \vdash \neg F$
3. $\exists x.(F(x) \vee G(x)) \vdash \exists x.F(x) \vee \exists x.G(x)$

Réponses

1.

$$\dfrac{\dfrac{}{((F \to G) \to H) \vdash ((F \to G) \to H)}\,Ax \qquad \dfrac{\dfrac{\dfrac{}{F \wedge G, F \vdash F \wedge G}\,Ax}{F \wedge G, F \vdash G}\,\wedge e2}{F \wedge G \vdash F \to G}\,\to i}{((F \to G) \to H); (F \wedge G) \vdash H}\,\to e$$

2.

$$\dfrac{\dfrac{}{\neg G \vdash \neg G}\,Ax \qquad \dfrac{\dfrac{}{F \to G \vdash F \to G}\,Ax \qquad \dfrac{}{F \vdash F}\,Ax}{(F \to G); F \vdash G}\,\to e}{(F \to G); \neg G; F \vdash \bot}\,\neg e$$
$$\dfrac{}{(F \to G); \neg G \vdash \neg F}\,\neg i$$

3.

$$\dfrac{\dfrac{\dfrac{}{\exists x.(F(x) \vee G(x)) \vdash \exists x.(F(x) \vee G(x))}\,Ax}{\exists x.(F(x) \vee G(x)) \vdash F(x) \vee G(x)}\,\exists e \qquad \dfrac{\dfrac{\dfrac{}{F(x_0) \vdash F(x_0)}\,Ax}{F(x_0) \vdash \exists x.F(x)}\,\exists i}{F(x_0) \vdash \exists x.F(x) \vee \exists x.G(x)}\,\vee i1 \qquad \dfrac{\dfrac{\dfrac{}{G(x_0) \vdash G(x_0)}\,Ax}{G(x_0) \vdash \exists x.G(x)}\,\exists i}{G(x_0) \vdash \exists x.F(x) \vee \exists x.G(x)}\,\vee i2}{\exists x.(F(x) \vee G(x)) \vdash \exists x.F(x) \vee \exists x.G(x)}\,\vee e$$

Question (III.2) Nous allons montrer que la formule $((F \to G) \to F) \to F$ est prouvable en déduction naturelle.

1. Donnez une preuve en déduction naturelle du séquent $\neg F \vdash F \to G$.
2. En déduire une preuve en déduction naturelle du séquent $((F \to G) \to F); \neg F \vdash F$.
3. En déduire une preuve en déduction naturelle de $\vdash ((F \to G) \to F) \to F$.

Réponses

1.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg F \vdash \neg F}\,Ax \qquad \dfrac{}{F \vdash F}\,Ax}{\neg F; F; G \vdash \bot}\,\neg e + Aff}{\neg F; F \vdash G}\,Abs}{\neg F \vdash F \to G}\,\to i$$

2.

$$\dfrac{\dfrac{}{(F \to G) \to F \vdash (F \to G) \to F}\,Ax \quad \dfrac{(1.)}{\neg F \vdash F \to G}}{((F \to G) \to F); \neg F \vdash F}\,{\to}e$$

3.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg F \vdash \neg F}\,Ax \quad \dfrac{(2.)}{(F \to G) \to F; \neg F \vdash F}}{(F \to G) \to F; \neg F \vdash \bot}\,\neg e}{(F \to G) \to F \vdash F}\,Abs}{\vdash ((F \to G) \to F) \to F}\,{\to}i$$

Exercice IV : *Système T*

Question (IV.1) Donnez la définition du terme *even* tel que

$$\begin{array}{lcl} (even\ \mathsf{S}^{2n}\mathsf{0}) & \hookrightarrow & \mathsf{S0} \\ (even\ \mathsf{S}^{2n+1}\mathsf{0}) & \hookrightarrow & \mathsf{0} \end{array}$$

On aura, en particulier que

$$\begin{array}{lcl} (even\ \mathsf{0}) & \hookrightarrow & \mathsf{S0} \\ (even\ \mathsf{S0}) & \hookrightarrow & \mathsf{0} \end{array}$$

Réponses

La fonction demandée décide si son argument est pair ou non (avec $\mathsf{S0}$ pour vrai et $\mathsf{0}$ pour faux). On sait que $\mathsf{0}$ est pair et que $\mathsf{S}x$ est pair si x ne l'est pas. On a donc $(even\ \mathsf{S}x) = not(even\ x)$ avec *not*, le terme $\lambda x.(if\ x\ \mathsf{0}\ x)$ vu en cours. Pour obtenir toujours $\mathsf{0}$ ou $\mathsf{S0}$ on redéfinit *not* comme $\lambda x.(if\ x\ \mathsf{0}\ \mathsf{S0})$. On pose alors

$$even = \lambda x.(\mathsf{rec}\ x\ \mathsf{S0}\ \lambda p \lambda h.(not\ h))$$

Une autre idée consiste à observer que $(even\ \mathsf{SS}x) = (even\ x)$. On retrouve alors une récurrence d'ordre 2, comme avec Fibonnacci. Et comme pour Fibonnacci, on peut construire la suite de couples $\langle (even\ x), (even\ \mathsf{S}x)\rangle$, C'est ici la suite

$$\langle \mathsf{S0}, \mathsf{0}\rangle\langle \mathsf{0}, \mathsf{S0}\rangle\langle \mathsf{S0}, \mathsf{0}\rangle\langle \mathsf{0}, \mathsf{S0}\rangle \ldots$$

On remarque que si le nième terme, C_n est $\langle t_1, t_2\rangle$ alors, le (n+1)-ième, C_{n+1} est $\langle t_2, t_1\rangle$; c'est-à-dire, $C_{n+1} = \langle \pi_2 C_n, \pi_1 C_n\rangle$. On définit alors le terme *enven*2 qui calcule le couple :

$$even2 = \lambda x.(\mathsf{rec}\ x\ \langle \mathsf{S0}, \mathsf{0}\rangle\ \lambda p \lambda h.\langle \pi_2 h, \pi_1 h\rangle)$$

et on pose que

$$even = \lambda x.\pi_1(even2\ x)$$
