Sécurité logicielle (HAI821I)

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

TD/TP N°1 : Preuves en logique du premier ordre

Exercice 1 (Logique propositionnelle)

Démontrer les propositions suivantes dans LJ et LK :

1. $A \Rightarrow B \Rightarrow A$
2. $(A \Rightarrow B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow A \Rightarrow C$
3. $A \wedge B \Rightarrow B$
4. $B \Rightarrow A \vee B$
5. $(A \vee B) \Rightarrow (A \Rightarrow C) \Rightarrow (B \Rightarrow C) \Rightarrow C$
6. $A \Rightarrow \bot \Rightarrow \neg A$
7. $\bot \Rightarrow A$
8. $(A \Leftrightarrow B) \Rightarrow A \Rightarrow B$
9. $(A \Leftrightarrow B) \Rightarrow B \Rightarrow A$
10. $(A \Rightarrow B) \Rightarrow (B \Rightarrow A) \Rightarrow (A \Leftrightarrow B)$

Exercice 2 (Logique du premier ordre)

Démontrer les propositions suivantes dans LJ et LK (si la proposition n'admet pas de preuve intuitionniste, démontrer la proposition dans $\mathrm{LJ}_{(\mathsf{em})}$) :

1. $\forall x.P(x) \Rightarrow \exists y.P(y) \vee Q(y)$
2. $(\exists x.P(x) \vee Q(x)) \Rightarrow (\exists x.P(x)) \vee (\exists x.Q(x))$
3. $(\forall x.P(x)) \wedge (\forall x.Q(x)) \Rightarrow \forall x.P(x) \wedge Q(x)$
4. $(\forall x.P(x) \wedge Q(x)) \Rightarrow (\forall x.P(x)) \wedge (\forall x.Q(x))$
5. $(\forall x.\neg P(x)) \Rightarrow \neg(\exists x.P(x))$
6. $\neg(\forall x.P(x)) \Rightarrow \exists x.\neg P(x)$

Exercice 3 (Preuves en Coq)

Démontrer les propositions des exercices 1 et 2 en Coq.

On rappelle que pour lancer Coq, il suffit de se mettre dans un terminal et de taper la commande `coqide`, qui lance l'IDE de Coq.

Exercice 4 (Preuves supplémentaires en Coq)

Démontrer les propositions suivantes en Coq (certaines preuves sont classiques) :

1. $(\exists x.\forall y.R(x,y)) \Rightarrow \forall y.\exists x.R(x,y)$
2. $(\forall x.\forall y.R(x,y)) \Rightarrow \forall x.\forall y.R(y,x)$
3. $(\exists x.\exists y.R(x,y)) \Rightarrow \exists y.\exists x.R(x,y)$
4. $(\exists x.\forall y.R(x,y)) \Rightarrow \forall y.\exists x.R(x,y)$
5. $\forall x.(\forall y.P(y) \Rightarrow P(x)) \Rightarrow (\exists y.P(y)) \Rightarrow P(x)$
6. $\exists x.P(x) \Rightarrow P(a) \wedge P(b)$
7. $\exists x.P(x) \Rightarrow P(a) \wedge P(b) \wedge P(c)$
8. $\exists x.P(x) \Rightarrow \forall y.P(y)$
9. $(\exists x.Q(a) \Rightarrow P(x)) \Rightarrow Q(a) \Rightarrow \exists x.P(x)$
10. $(Q(a) \Rightarrow \exists x.P(x)) \Rightarrow \exists x.Q(a) \Rightarrow P(x)$