	Année 2018/2019	TD Preuve formelle

LOGIQUE ET PREUVE DE PROGRAMMES
IF107

Filière : Informatique, Année : 1
Web: `http://herbrete.vvv.enseirb-matmeca.fr/IF107`

1 Un calcul simple

Soit N l'ensemble des mots constitués d'une séquence non vide de symboles $\bullet$. Intuitivement N représente les entiers naturels *non nuls* en base unaire : $\bullet$ représente 1, $\bullet\bullet$ représente 2, $\bullet\bullet\bullet$ représente 3, etc. Dans la suite, x et y représentent deux mots de N. On note $n(x)$ et $n(y)$ les nombres qu'ils représentent (i.e. leur longueur). Leur concaténation xy représente donc la somme : $n(xy) = n(x) + n(y)$.

Exercice 1 (La règle NDP)

On considère dans un premier temps le système formel constitué de l'axiome (Ax) et de la règle de déduction (R_1) ci-dessous, où la proposition $''x\,NDP\,y''$ se lit $''x$ Ne Divise Pas y''.

$$\frac{}{xy\,NDP\,x}\ (Ax) \qquad\qquad \frac{x\,NDP\,y}{x\,NDP\,xy}\ (R_1)$$

1. Prouver la proposition $\bullet\bullet\ NDP\ \bullet\bullet\bullet$ dans ce système formel
2. Que se passe-t-il si on tente de prouver une proposition invalide comme $\bullet\bullet\ NDP\ \bullet\bullet\bullet\bullet$?
3. Montrer *par induction*[1] que $x\,NDP\,y$ est prouvable si et seulement si $n(x)$ ne divise pas $n(y)$.

♦

Exercice 2 (La règle SD)

On ajoute maintenant les règles (R_2) et (R_3) ci-dessous au système formel précédent, où la proposition $''x\,SD\,y''$ se lit $''x$ est Sans Diviseur entre 2 (i.e. $\bullet\bullet$) et y''.

$$\frac{\bullet\bullet\,NDP\,x}{x\,SD\,\bullet\bullet}\ (R_2) \qquad\qquad \frac{x\bullet\,NDP\,y \qquad y\,SD\,x}{y\,SD\,x\bullet}\ (R_3)$$

1. Donner une preuve qui montre la validité de $\bullet\bullet\bullet\bullet\bullet\,SD\ \bullet\bullet\bullet$
2. Montrer *par induction* que si $x\,SD\,y$ est prouvable, alors $n(x)$ n'admet aucun diviseur entre 2 et $n(y)$.

♦

1. La preuve par induction d'une propriété P pour une règle R consiste à montrer que P est vraie pour la conclusion de R en supposant que P est vraie pour les prémisses de R.

Exercice 3 **(La règle P)**

On ajoute finalement l'axiome (Ax) et la règle (R_4) ci-dessous au système formel précédent, où la proposition $''P\,x''$ se lit $''x$ est Premier''.

$\frac{}{P\,\bullet\bullet}$ (Ax_2) $\frac{x\bullet\,SD\,x}{P\,x\bullet}$ (R_4)

1. Donner une preuve qui montre la validité de $P\ \bullet\bullet\bullet$.
2. Montrer *par induction* que si $P\,x$ est prouvable, alors $n(x)$ est un nombre premier.

♦

Cette séquence d'exercices (tirée du sujet d'examen 2010/2011) est inspirée de "Gödel, Escher et Bach, les brins d'une guirlande éternelle", D. Hofstadter, Inter éditions, 1993.

2 Calcul des séquents propositionnel

1. utilisation d'une hypothèse : $\dfrac{}{\Gamma, \psi \vdash \psi}$
2. augmentation des hypothèses : $\dfrac{\Gamma \vdash \phi \quad \psi \notin \Gamma}{\Gamma, \psi \vdash \phi}$
3. détachement (Modus ponens) : $\dfrac{\Gamma \vdash (\phi \implies \phi') \quad \Gamma \vdash \phi}{\Gamma \vdash \phi'}$
4. retrait d'une hypothèse : $\dfrac{\Gamma, \psi \vdash \phi}{\Gamma \vdash (\psi \implies \phi)}$
5. double négation : $\dfrac{\Gamma \vdash \phi}{\Gamma \vdash \neg\neg\phi}$ $\qquad \dfrac{\Gamma \vdash \neg\neg\phi}{\Gamma \vdash \phi}$
6. contradiction : $\dfrac{\Gamma, \psi \vdash \phi \qquad \Gamma, \psi \vdash \neg\phi}{\Gamma \vdash \neg\psi}$
7. conjonction : $\dfrac{\Gamma \vdash \phi \qquad \Gamma \vdash \phi'}{\Gamma \vdash (\phi \wedge \phi')}$ $\qquad \dfrac{\Gamma \vdash (\phi \wedge \phi')}{\Gamma \vdash \phi}$ $\qquad \dfrac{\Gamma \vdash (\phi \wedge \phi')}{\Gamma \vdash \phi'}$
8. disjonction : $\dfrac{\Gamma, \psi \vdash \phi \qquad \Gamma, \neg\psi \vdash \phi'}{\Gamma \vdash (\phi \vee \phi')}$ $\qquad \dfrac{\Gamma, \psi \vdash \phi \qquad \Gamma, \psi' \vdash \phi}{\Gamma, (\psi \vee \psi') \vdash \phi}$

Exercice 4 **(Premières preuves)**

Montrer que les séquents suivants sont prouvables. Pour chacun des séquents, indiquer quelle formule est prouvée valide.

1. $A, B \vdash (A \wedge B)$
2. $A, (A \implies B) \vdash B$
3. $A, B, (A \implies B \implies C) \vdash C$
4. $(A \vee B), (A \implies C), (B \implies C) \vdash C$

♦

Exercice 5 **(Lemmes)**

Démontrer les règles suivantes à l'aide du calcul des séquents propositionnel.

1. $\dfrac{\Gamma, \psi, \psi' \vdash \phi}{\Gamma, (\psi \wedge \psi') \vdash \phi}$
2. $\dfrac{\Gamma, (\psi \wedge \psi') \vdash \phi}{\Gamma, \psi, \psi' \vdash \phi}$
3. Modus tollens : $\dfrac{\Gamma \vdash \neg\phi' \quad \Gamma \vdash (\phi \implies \phi')}{\Gamma \vdash \neg\phi}$

♦

Exercice 6 **(Equivalences logiques standards)**

Définir les séquents à prouver pour démontrer chacun des équivalences logiques ci-dessous. Donner une preuve pour chacun de ces séquents.

1. $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$
2. $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$
3. $\neg(A \vee B) \equiv \neg A \wedge \neg B$
4. $\neg(A \wedge B) \equiv \neg A \vee \neg B$
5. $A \Rightarrow B \equiv \neg A \Rightarrow \neg B$
6. $A \implies B \equiv \neg A \vee B$

♦

3 Calcul des séquents en logique des prédicats

Régles du calcul propositionnel, plus les règles ci-dessous pour les quantificateurs :

9. introduction : $\dfrac{\Gamma \vdash \phi}{\Gamma \vdash \forall x.\phi}$ **avec** x **non libre dans** Γ $\qquad \dfrac{\Gamma \vdash \phi[x \leftarrow t]}{\Gamma \vdash \exists x.\phi}$
10. élimination : $\dfrac{\Gamma \vdash \forall x.\phi}{\Gamma \vdash \phi[x \leftarrow t]}$ $\qquad \dfrac{\Gamma \vdash \exists x.\phi \quad \Gamma, \phi \vdash \psi}{\Gamma \vdash \psi}$ **avec** x **non libre dans** Γ **et** Ψ

où t est un terme quelconque (une valeur quelconque de x) et $\phi[x \leftarrow t]$ est la substitution de t à x dans ϕ.

Exercice 7 **(Preuve en séquents des prédicats)**

Soit R un symbole de relation binaire.

1. formaliser en logique des prédicats : R est totale, R est symmétrique, R est transitive et R est réflexive
2. formaliser par un séquent la proposition suivante : ”si R est totale, symmétrique et transitive, alors R est réflexive”
3. pouver le séquent ci-dessus

♦