Université Bordeaux 1
Mastère d'Informatique 1, 2008/2009

LOGIQUE, INF 462

Examen du 19/12/2008
Sujet de M. Sénizergues ; tous documents autorisés ; durée conseillée : 1h 30.

Exercice 4 (sur 4 points)
Donner des preuves dans LK des séquents :

$$S_1 : \quad \exists x(P(x) \wedge Q(x)) \vdash (\exists x P(x)) \wedge (\exists x Q(x))$$
$$S_2 : \quad \forall x(P(x) \wedge Q(x)) \vdash (\forall x P(x)) \wedge (\forall x Q(x))$$

Exercice 5 (sur 2 points)
On considère l'arbre de séquents suivant, où $\mathtt{ax}'$ désigne un axiome suivi d'un affaiblissement :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P(x) \vdash P(x), Q(x)}\,\mathtt{ax}' \qquad \dfrac{}{Q(x) \vdash P(x), Q(x)}\,\mathtt{ax}'}{P(x) \vee Q(x) \vdash P(x), Q(x)}\,?\ \vee g}{\forall x(P(x) \vee Q(x)) \vdash P(x), Q(x)}\,?\ \forall g}{\forall x(P(x) \vee Q(x)) \vdash (\forall x P(x)), Q(x)}\,?\ \forall d}{\forall x(P(x) \vee Q(x)) \vdash (\forall x P(x)), (\forall x Q(x))}\,?\ \forall d}{\forall x(P(x) \vee Q(x)) \vdash (\forall x P(x)) \vee (\forall x Q(x))}\,?\ \vee d$$

1- S'agit-il d'une preuve dans LK ? Si oui, préciser quelle règle est utlilisée à chaque noeud ; si non, préciser quel noeud ne correspond à aucune règle.
2- Existe-t-il des exemples de prédicats P et Q tels que le séquent $\forall x\big(P(x) \vee Q(x)\big) \vdash (\forall x P(x)) \vee (\forall x Q(x))$ ne soit pas valide ?

Exercice 6 (sur 4 points)
Deux propositions A et B sont *équivalentes* dans LJ (notation $A \equiv_{\mathrm{LJ}} B$) si les séquents $A \vdash B$ et $B \vdash A$ y sont dérivables. Montrer les équivalences suivantes :

$$(A \wedge B) \rightarrow C \equiv_{\mathrm{LJ}} A \rightarrow (B \rightarrow C), \tag{1}$$
$$A \rightarrow (B \wedge C) \equiv_{\mathrm{LJ}} (A \rightarrow B) \wedge (A \rightarrow C). \tag{2}$$

En déduire l'équivalence suivante :

$$A \rightarrow \big(B \rightarrow (C \wedge D)\big) \equiv_{\mathrm{LJ}} \big((A \wedge B) \rightarrow C\big) \wedge \big((A \wedge B) \rightarrow D\big). \tag{3}$$

En construisant une structure de Kripke bien choisie, montrer que l'équivalence suivante n'est pas vraie :

$$[A \rightarrow (B \vee C)] \equiv_{\mathrm{LJ}} [(A \rightarrow B) \vee (A \rightarrow C)] \tag{4}$$

Université Bordeaux 1. Master d'informatique.
Logique INF462

19 Décembre 2007

Sujet de M. Castéran   Tous documents autorisés ; durée conseillée : 1h30

À lire avant d'écrire quoi que ce soit *Le critère d'évaluation sera la qualité et la clarté de vos explications. Les commandes* Coq *non accompagnées d'explications ne seront pas prises en compte ; il vaut mieux expliquer simplement la structure de vos preuves ; par exemple vous pouvez donner des explications de la forme* « En appliquant telle tactique, les nouveaux buts suivants sont engendrés ». *On peut aussi présenter les démonstrations sous forme de déduction naturelle.*

1 Exercice (3pts / 10)

On considère trois variables `P`, `Q` et `R` de type `Prop`. Donner des preuves (sans utiliser de tactique automatique) des énoncés suivants :

`((P → Q) → R) → Q → R`

`(P → ~P) → ~P`

`(P ∨ ~Q) → (P → R) → Q → R.`

2 Exercice (2 pts / 10)

On considère les déclarations suivantes :

```
Parameter A:Set.
Parameter P:A → Prop.
Parameter a:A.
```

Montrer les deux implications suivantes :

`P a → ∃x:A, x=a ∧ P x`

`(∃x:A, x=a ∧ P x) →P a`

3 Problème (5 pts / 10)

On se réfère au fichier donné en Annexe. *Tous les résultats admis dans ce fichier peuvent être utilisés ; les sections 3.1 et 3.2 sont indépendantes.*

3.1

Comment énoncer et prouver que 3 n'est pas un nombre pair ?

3.2

On veut prouver le lemme suivant :

```
Lemma Even_half : ∀n:Nat, Even n → ∃p:Nat, n = p + p.
```

3.2.1

Le premier réflexe est de tenter le début de preuve suivant :

```
Proof.
 intro n.
 induction n using Nat_ind.
```

Quels sont les sous-buts engendrés ? Expliquer. Peut-on terminer la preuve ? Pourquoi ?

3.2.2

On a une autre idée, et on recommence :

```
Lemma Even_half : ∀ n:Nat, Even n → ∃p:Nat, n = p + p.
Proof.
 intros  n H.
 induction H using Even_ind.
```

Quels sont les sous-buts engendrés ? Expliquer. Peut-on terminer la preuve ? Comment ?

4 Annexe : Sources Coq pour le problème

```
Parameter Nat : Set.
Parameter zero : Nat.
Parameter S : Nat -> Nat.
Parameter plus : Nat -> Nat -> Nat.

Notation "n + p" := (plus n p).
```

```
(* Axiomes (sont des theoremes dans la bibliotheque standard de Coq) *)

Axiom zero_not_S : forall n:Nat, S n <> zero.
Axiom S_injective : forall n p, S n = S p -> n = p.
Axiom zero_plus_n : forall n:Nat, zero + n = n.
Axiom S_plus_n : forall n p:Nat, S n + p = S (n + p).

(* axiome de recurrence *)

Axiom Nat_ind : forall (P:Nat->Prop), P zero ->
                                      (forall p:Nat, P p -> P (S p)) ->
                                      forall n:Nat, P n.

Hint Resolve zero_not_S S_injective zero_plus_n S_plus_n.

Lemma fib_ind : forall (P:Nat->Prop),
                P zero -> P (S zero) ->
                (forall p : Nat, P p -> P (S (S p))) ->
                forall n : Nat, P n.
Admitted.

Lemma zero_or_S : forall n:Nat, n=zero \/ exists p:Nat, n = S p.
Admitted.

(* Proprietes de l'addition *)

Lemma n_plus_zero : forall n:Nat, n + zero =n.
Admitted.

Hint Rewrite n_plus_zero zero_plus_n S_plus_n : peano.

Lemma n_plus_S : forall n p:Nat, n+ S p = S(n+p).
Admitted.

Hint Rewrite n_plus_S :peano.
Hint Resolve n_plus_S n_plus_zero.

Theorem plus_comm : forall n p:Nat, n + p = p + n.
Admitted.

Theorem plus_assoc : forall n p q:Nat, (n+p)+q = n+(p+q).
Admitted.

Hint Rewrite plus_assoc :peano.

(* Debut des nouvelles definitions *)
```

```
Parameter Even : Nat -> Prop.

Axiom Even_zero : Even zero.

Axiom Even_S_S : forall n:Nat, Even n -> Even (S (S n)).

Axiom Even_ind : forall (P:Nat->Prop),
   P zero ->
   (forall n :  Nat, Even n -> P n -> P (S (S n))) ->
   forall n:Nat, Even n -> P n.

Definition Odd n := Even (S n).

Lemma Even_inv : forall n, Even n ->
                   n=zero \/ exists q:Nat, n=S (S q) /\ Even q.
Admitted.

Lemma not_Even_1 : ~ Even (S zero).
Admitted.

Lemma Even_S_S_inv : forall n:Nat, Even (S (S n)) -> Even n.
Admitted.
```

Université Bordeaux 1
Mastère d'Informatique 1, 2008/2009

LOGIQUE

TD7 : Calcul des séquents

Symétries du système LK

Exercice 7.1 Réversibilité

Une règle d'inférence $\frac{S_1}{S_2}$ d' un système formel $\mathcal{S}$ est dite *réversible* si $\frac{S_2}{S_1}$ est une règle dérivée du système $\mathcal{S}$. Quelles sont les règles réversibles du système LK ?

Exercice 7.2 Dualité $\top$ = true

On ajoute le connecteur $\top$ au langage du système LK i.e. l'ensemble des connecteurs $\{\bot, \wedge, \vee, \rightarrow, \neg\}$, l'ensemble de quantificateurs $\{\forall, \exists\}$, un ensemble dénombrable de symboles de relations $\mathcal{R}$ et un ensemble dénombrable de symboles de fonctions $\mathcal{F}$.

Pour toute formule F bien-formée on définit la formule duale $\mathrm{D}(F)$ par induction structurelle :

$$\mathrm{D}(\bot) := \top, \quad \mathrm{D}(\top) := \bot$$

$$\mathrm{D}(R(t_1, \ldots, t_k)) := R(t_1, \ldots, t_k) \quad \text{pour tout } R \in \mathcal{R}$$

$$\mathrm{D}(F \wedge G) := \mathrm{D}(F) \vee \mathrm{D}(G), \quad \mathrm{D}(F \vee G) := \mathrm{D}(F) \wedge \mathrm{D}(G)$$

$$\mathrm{D}(F \rightarrow G) := \neg(\mathrm{D}(G) \rightarrow \mathrm{D}(F)), \quad \mathrm{D}(\neg F) := \neg \mathrm{D}(F)$$

$$\mathrm{D}(\forall x F) := \exists x \mathrm{D}(F), \quad \mathrm{D}(\exists x F) := \forall x \mathrm{D}(F)$$

1- Montrer que pour toute formule F, dont les sous-formules atomiques sont $A_1, \ldots, A_n$, on a l'équivalence :

$$F(\neg A_1, \ldots, \neg A_n) \models\!\!\!\!\mid\; \neg \mathrm{D}(F)(A_1, \ldots, A_n).$$

On étend naturellement l'application $F \mapsto \mathrm{D}(F)$ aux séquents en posant :

$$\mathrm{D}(F_1, \ldots, F_n \vdash G_1 \ldots, G_m) := \mathrm{D}(G_1), \ldots, \mathrm{D}(G_m) \vdash \mathrm{D}(F_1), \ldots, \mathrm{D}(F_n).$$

2- Montrer que si, pour toute structure $\mathcal{T}$ et toute valuation v on a :

$$(\mathcal{T}, v) \models S_1 \text{ implique } (\mathcal{T}, v) \models S_2$$

alors, pour toute structure $\mathcal{T}$ et toute valuation v on a aussi :

$$(\mathcal{T}, v) \models \mathrm{D}(S_1) \text{ implique } (\mathcal{T}, v) \models \mathrm{D}(S_2).$$

3- Quelles sont les règles $\frac{S_1}{S_2}$ (où S_1 est un séquent ou bien le mot vide, et S_2 est un séquent) de LK telles que $\frac{\mathrm{D}(S_1)}{\mathrm{D}(S_2)}$ est encore une règle ?

4- Ajouter une règle à LK de façon à l'adapter à l'ajout du connecteur $\top$. On voudrait que le séquent $\vdash (\neg\bot \rightarrow \top) \wedge (\top \rightarrow \neg\bot)$ soit prouvable dans cette extension de LK et on souhaite conserver (ou améliorer) les propriétés de symétrie de LK.

Exemples de preuves

Exercice 7.3 LK propositionnel

Donner une preuve dans LK des séquents :

$\vdash A \rightarrow (B \rightarrow A)$

$\vdash (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$

$\vdash ((P \rightarrow Q) \rightarrow P) \rightarrow P$

Exercice 7.4 LK

Donner une preuve dans LK des séquents :

$\neg\exists x R(x) \vdash \forall x \neg R(x)$

$\neg\forall x R(x) \vdash \exists x \neg R(x)$

$\vdash \forall x(Q \vee R(x)) \rightarrow Q \vee \forall x R(x)$

$\vdash \exists x \forall y (R(y) \rightarrow R(x))$

Exercice 7.5 LJ propositionnel

Donner une preuve dans LJ des séquents :

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

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

$A \vdash \neg\neg A$

$\neg\neg\neg A \vdash \neg A$

Exercice 7.6 LJ

1- Que pensez-vous de la “preuve” suivante ?

$$\begin{array}{ll}
R(x) \vdash R(x) & \texttt{ax} \\
\exists x R(x) \vdash R(x) & \exists_g \leftarrow x \in VL(R(x)) \\
\neg R(x), \exists x R(x) \vdash & \neg_g \\
\forall x \neg R(x), \exists x R(x) \vdash & \forall_g \\
\forall x \neg R(x) \vdash \neg\exists x R(x) & \neg_d
\end{array}$$

2- Le séquent $\forall x \neg R(x) \vdash \neg\exists x R(x)$ est-il prouvable dans LJ ?

Propriétés des preuves

Exercice 7.7 Elimination à droite

On sonsidère la règle suivante (d'élimination à droite) :

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}$$

(où Γ est un multi-ensemble de formules et A, B sont des formules).

1- Cette règle est-elle dérivable dans LK ?

2- Cette règle est-elle dérivable dans LK privé de la règle de coupure ?

Exercice 7.8 Contractions

On considère le séquent $S := \exists x(R(a) \vee R(b) \rightarrow R(x))$.

1- Donner une preuve de S dans LK.

2- Donner une preuve sans coupure de S dans LK.

3- Montrer qu'il n'existe pas de preuve sans coupure ni contraction de S dans LK.

Université Bordeaux 1
Mastère d'Informatique 1, 2008/2009

LOGIQUE

TD8 : Élimination des coupures

Exercice 8.1 Harrop

1- On considère les théories (i.e. ensembles de formules) : $\mathrm{EG}, \mathrm{P}_0, \mathrm{PA}, \mathrm{MO}, \mathrm{GR}$. Lesquelles sont des théories de Harrop ? Quelles conséquences peut-on en tirer ?

Exercice 8.2 PA versus P_0

1-Notons P'_0 (resp. PA') l'ensemble des formules de P_0 (resp. PA) sauf l'axiome A2. PA' est-il une théorie de Harrop ?

2- Donner une preuve dans LK de $\mathrm{PA}' \vdash A2$.

3- Pouvez-vous donner une preuve dans LJ de $\mathrm{PA}' \vdash A2$? existe-t-il un terme t, et une preuve dans LK de $\mathrm{PA}' \vdash \ x = 0 \vee x = S(t)$?

Exercice 8.3 Un modèle non-standard de P'_0.

Soit $\mathcal{M} =_{\text{déf.}} \langle \mathcal{N}, 0_{\mathcal{N}}, \mathrm{S}_{\mathcal{N}}, +_{\mathcal{N}}, \times_{\mathcal{N}} \rangle$ la structure « arithmétique » suivante :

$$\begin{aligned}
\mathcal{N} &=_{\text{déf.}} (\mathbb{N} \times \{\bullet\}) \cup (\mathbb{N} \times \{\circ\}) \text{ où } \bullet \neq \circ \\
0_{\mathcal{N}} &=_{\text{déf.}} \langle 0, \bullet \rangle \\
\mathrm{S}_{\mathcal{N}}\langle p, \alpha \rangle &=_{\text{déf.}} \langle \mathrm{S}p, \alpha \rangle \text{ où } \alpha \in \{\bullet, \circ\} \\
\langle p, \alpha \rangle +_{\mathcal{N}} \langle q, \beta \rangle &=_{\text{déf.}} \langle p + q, \alpha \rangle \text{ où } \alpha, \beta \in \{\bullet, \circ\} \\
\langle p, \alpha \rangle \times_{\mathcal{N}} \langle q, \beta \rangle &=_{\text{déf.}} \langle p \times q, \beta \rangle \text{ où } \alpha, \beta \in \{\bullet, \circ\}
\end{aligned}$$

Le domaine $\mathcal{N}$ est constitué de deux copies de $\mathbb{N}$, les entiers « noirs » $\langle p, \bullet \rangle$ et les entiers « blancs » $\langle p, \circ \rangle$.La constante zéro est interprétée par le zéro noir $\langle 0, \bullet \rangle$; les opérations successeur, addition et multiplication sont interprétées de telle sorte que :

- le successeur conserve la couleur de son argument,
- l'addition prend la couleur de son *premier* argument,
- la multiplication prend la couleur de son *second* argument.

1. Montrer que $\mathcal{M}$ est un modèle de P'_0. Est-ce un modèle de P_0 ?
2. Montrer qu'aucune des propriétés suivantes n'est conséquence de P'_0 :

$$\forall x \ (0 + x = x) \tag{1}$$
$$\forall x, y \ (x + y = y + x) \tag{2}$$
$$\forall x, y, z \ (x + y = x + z \to y = z) \tag{3}$$
$$\forall x \ (x \times \mathrm{S}0 = x) \tag{4}$$
$$\forall x, y \ (x \times y = y \times x) \tag{5}$$

Exercice 8.4 Arithmétique de Heyting

Soit Φ une formule du premier ordre sur la signature de l'arithmétique.

1- Montrer que , si $\mathrm{P}'_0 \vdash \ \forall x \Phi$ est prouvable dans LJ, alors $\mathrm{P}'_0 \vdash \ \Phi$ est prouvable dans LJ.

2- La propriété de la question 1 est-elle vraie en prenant comme membre gauche PA ? ou en prenant comme système logique LK ?

3- Montrer que, si $\mathrm{P}'_0 \vdash \forall x, \exists y \Phi(x, y)$ est prouvable dans LJ, alors, il existe un terme t tel que $\mathrm{P}'_0 \vdash \Phi(x, t)$ est prouvable dans LJ.

4- La propriété de la question 3 est-elle vraie en prenant comme membre gauche PA ? ou en prenant comme système logique LK ?

5- Supposons que $\mathrm{PA}' \vdash \forall x, \exists y \Phi(x, y)$ est prouvable dans LJ, en " n'utilisant qu'une seule récurrence" i.e.

$$\mathrm{P}'_0 \vdash_{\mathrm{LJ}} \exists y \ \ \Phi(0, y); \quad \mathrm{P}'_0 \vdash_{\mathrm{LJ}} (\exists y \Phi(x, y)) \rightarrow (\exists y \Phi(S(x), y))$$

5.1- Vérifer que, sous ces hypothèses, il existe bien dans LJ une preuve de $\mathrm{PA}' \vdash \forall x, \exists y \Phi(x, y)$.
Pour tout $n \in \mathbb{N}$, on note $\underline{n}$ le terme $S(S(\ldots(S(0))\ldots))$ qui reprénte l'entier n dans le langage de l' arithmétique de Peano.

5.2- Montrer que, pour tout entier $n \in \mathbb{N}$, il existe un terme t_n tel que $\mathrm{P}'_0 \vdash_{\mathrm{LJ}} \Phi(\underline{n}, t_n)$.

5.3- Donner un algorithme de calcul de la fonction $n \mapsto t_n$ fondé sur l'algorithme d'élimination des coupures.

On admet maintenant que la propriété démontré dans l'exercice 4, question 5, est vraie pour toute formule de la forme $\forall x, \exists y \Phi(x, y)$ (même si la preuve utilise plus qu'une récurrence).

Exercice 8.5 Fonctions récursives

On se demande si une réciproque de l'énoncé admis ci-dessus est vraie. Nous faisons la supposition (**SUPP**) :
pour toute fonction totale, calculable, $f : \mathbb{N} \rightarrow \mathbb{N}$, il existe une formule $\Phi(x, y)$ telle que
(P1) $\mathrm{PA} \vdash \forall x, \exists_1 y \Phi(x, y)$ est prouvable dans LJ
où $\exists_1 x \ \ F(x)$ est une abbréviation de $\exists x \ \ F(x) \wedge (\forall y, z \ \ F(y) \wedge F(z) \rightarrow y = z)$
(P2) pour tous entiers naturels n, m, $\mathbb{N} \models \ \Phi(\underline{n}, \underline{m})$ si et seulement si $f(n) = m$.

1- Peut-on en déduire une énumération effective des fonctions totales calculables ?

2- Par un argument de diagonalisation, montrer que **SUPP** est fausse.

Admettons le théorème [Matiyasevich, 1971] : une partie $M \subseteq \mathbb{N}$ est récursivement énumérable ssi, il existe un entier $q \in \mathbb{N}$ et un polynôme $P \in \mathbb{Z}[X, Y_1, \ldots, Y_q]$ tels que, pour tout $x \in \mathbb{N}$,

$$x \in M \Leftrightarrow \exists \vec{y} \in \mathbb{N}^q, P(x, \vec{y}) = 0.$$

Exercice 8.6 Indécidabilité de PA

Soit q un entier naturel, P un polynome de $\mathbb{Z}[X, Y_1, \ldots, Y_q]$.

1- Montrer que, si $\mathbb{N} \models \exists \vec{y} P(\underline{n}, \vec{y}) = 0$.
alors il existe un vecteur d'entiers naturels $\vec{m}$ tel que $\mathrm{PA} \vdash_{\mathrm{LK}} P(\underline{n}, \underline{\vec{m}}) = 0$.

2- Montrer que, si $\mathrm{PA} \vdash_{\mathrm{LK}} \exists \vec{y}\ P(\underline{n}, \vec{y}) = 0$, alors $\mathbb{N} \models \exists \vec{y} P(\underline{n}, \vec{y}) = 0$.

3- Montrer qu' il existe un polynôme P tel que le problème
Donnée : $n \in \mathbb{N}$; Question : existe-t-il un vecteur $\vec{m} \in \mathbb{N}^q$ tel que $P(n, \vec{m}) = 0$?
est indécidable.

4- En déduire que le problème suivant est indécidable :
Donnée : une formule Φ ; Question : $\mathrm{PA} \vdash_{\mathrm{LK}} \Phi$?

Exercice 8.7 Signature

Pour tout multi-ensemble de formules Γ, on note $\mathcal{S}(\Gamma)$ la signature composée des symboles de relation et des symboles de fonctions apparaissant dans Γ.

1- Montrer que, si le séquent $\Gamma \vdash \Delta$ est prouvable dans LK, alors il admet une preuve qui n'utilise que des symboles de $\mathcal{S}(\Gamma, \Delta)$.

2- Soit $S = \Gamma \vdash \Delta$ un séquent n'utilisant aucun symbole de fonction. Montrer qu'il existe un ensemble fini de formules $\mathcal{F}$, calculable à partir de S, tel que S est prouvable dans LK ssi il admet une preuve dont tous les séquents sont des paires $\Gamma' \vdash \Delta'$ où Γ', Δ' sont des multi-ensembles de formules de l'ensemble $\{F[x_1 := y_1, \ldots, x_q := y_q] \mid y_j \in \mathcal{V}, F \in \mathcal{F}\}$.

3- Peut-on en conclure que le problème suivant est décidable :
Donnée : un séquent $S = \Gamma \vdash \Delta$, sans symbole de fonction ; Question : S est-il dérivable dans LK ?

Exercice 8.8 Équations dans les groupes

1- Esquisser une preuve π_1 dans LJ de

$$\mathrm{GR} \vdash \exists x \quad x * a * a * b = b * a * a * x$$

2- Esquisser une preuve π_2 dans LJ de

$$\mathrm{GR}, x * a * a * b = b * a * a * x \vdash \exists y \;\; b * a * a * x * I(b) * I(a) * I(a) * x * x = y * y * I(x)$$

3- En déduire, en utilisant une coupure, une preuve dans LJ de

$$\mathrm{GR} \vdash \exists x \exists y \;\; b * a * a * x * I(b) * I(a) * I(a) * x * x = y * y * I(x)$$

4- Quels sont les termes t_1, t_2 fournis par π_1, π_2, tels que

$$\mathrm{GR} \vdash \quad t_1 * a * a * b = b * a * a * t_1$$

et

$$\mathrm{GR}, x * a * a * b = b * a * a * x \vdash \quad b * a * a * x * I(b) * I(a) * I(a) * x * x = t_2 * t_2 * I(x)$$

5- Pouvez-vous en déduire des termes t_3, t_4 tels que

$$\mathrm{GR} \vdash \quad b * a * a * t_3 * I(b) * I(a) * I(a) * t_3 * t_3 = t_4 * t_4 * I(t_3)$$

6- Comment obtenir de tels termes t_3, t_4 par élimination de coupures ?

Université Bordeaux 1
Mastère d'Informatique 1, 2008/2009

LOGIQUE

TD9 : Structures de Kripke

Exercice 9.1

Donner une preuve sémantique de $\Vdash \forall x \neg\neg(R(x) \vee \neg R(x))$

Exercice 9.2

1- Trouver une structure de Kripke $\mathcal{K}$ qui est un contre-modèle de

$$(\neg A \to B) \to (\neg B \to A)$$

2- Le séquent $\vdash (\neg A \to B) \to (\neg B \to A)$ est-il prouvable dans LK ? dans LJ ?

Exercice 9.3 LJ versus LK

On considère les séquents suivants qui sont prouvables dans LK (voir la feuille 7). Déterminer pour chacun d'eux s'il est prouvable dans LJ.

1- $\vdash (A \to (B \to C)) \to ((A \to B) \to (A \to C))$
2- $\vdash ((P \to Q) \to P) \to P$
3- $\vdash \neg\forall x \neg R(x) \to \exists x R(x)$
4- $\vdash \exists x \forall y (R(y) \to R(x))$
5- $\forall x \neg R(x) \vdash \neg\exists x R(x)$
6- $\vdash \exists x (R(a) \vee R(b) \to R(x))$.

Exercice 9.4 Bisimulations

Soient $\mathcal{K}_1, \mathcal{K}_2$ des structures de Kripke sur une signature propositionnelle $\mathcal{Q} = \{Q_1, \ldots, Q_n\}$. On note $\mathcal{K}_i = (K_i, \leq_i, \Vdash_i)$ pour $i \in \{1,2\}$. Une relation $R \subseteq K_1 \times K_2$ est une *bisimulation* ssi elle vérifie les trois propriétés B1,B2,B3 suivantes :

(B1) $\forall (k_1, k_2) \in R, \forall Q \in \mathcal{Q}, k_1 \Vdash Q \Leftrightarrow k_2 \Vdash Q$

(B2) $\forall (k_1, k_2) \in R, \forall k_2' \in K_2$ tel que $k_2 \leq_2 k_2'$,

$$\exists k_1' \in K_1 \text{ tel que } (k_1', k_2') \in R \ \& \ k_1 \leq_1 k_1'.$$

(B3) $\forall (k_1, k_2) \in R, \forall k_1' \in K_1$ tel que $k_1 \leq_1 k_1'$

$$\exists k_2' \in K_2 \text{ tel que } (k_1', k_2') \in R \ \& \ k_2 \leq_2 k_2'.$$

1- Montrer que si R est une bisimulation alors, pour tout $(k_1, k_2) \in R$ et pour toute formule A,

$$k_1 \Vdash_1 A \Leftrightarrow k_2 \Vdash_2 A.$$

2- Montrer que toute structure de Kripke possédant un plus petit élément est bisimilaire à un arbre.

Exercice 9.5 Une structure complète

Soit $\mathcal{K} = (K, \leq, \Vdash)$ une structure de Kripke sur la signature propositionnelle $\mathcal{Q}$ et A une formule sur $\mathcal{Q}$. On note $SF(A)$ l'ensemble des sous-formules de A. Pour tout $k \in K$ on note $S(k) := \{B \in SF(A) \mid k \Vdash B\}$. On définit une structure de Kripke $\mathcal{K}^* = (K^*, \leq^*, \Vdash^*)$ par :

$$K^* := \{S(k) \mid k \in K\}, \quad S(k) \leq^* S(k') \Leftrightarrow S(k) \subseteq S(k')$$

et pour tout $Q \in \mathcal{Q}$

$$S(k) \Vdash^* Q \Leftrightarrow Q \in S(k).$$

1- Montrer que, pour tout $B \in SF(A)$ et tout $k \in K$,

$$k \Vdash B \Leftrightarrow S(k) \Vdash^* B$$

2- En déduire une méthode sémantique permettant de tester, pour toute formule propositionnelle A si $\Vdash A$.

3- Montrer que, pour toute formule propositionnelle A , $\vdash_{\mathrm{LJ}} A$ ssi toute structure de Kripke finie $\mathcal{K}$ réalise A.

4- En utilisant l'exercice 9.4, montrer que, pour toute formule propositionnelle A , $\vdash_{\mathrm{LJ}} A$ ssi toute structure de Kripke $\mathcal{K}$ qui est un arbre fini réalise A.

5- Construire une structure de Kripke propositionnelle $\mathcal{K}$ sur $\mathcal{Q}$, qui est un arbre dénombrable et telle que, pour toute formule propositionnelle A sur $\mathcal{Q}$,

$$\vdash_{\mathrm{LJ}} A \Leftrightarrow \mathcal{K} \Vdash A.$$

$(P \to Q) \to (Q \to R) \to P \to R$

$P \to Q, Q \to R, P \vdash P \to Q$ $\Rightarrow$ var $\quad \ldots \vdash P$

$P \to Q, Q \to R, P \vdash Q \to R$ $\Rightarrow$ var $\quad P \to Q, Q \to R, P \vdash Q$ $\Rightarrow$ ~~var~~ mp

$P \to Q, Q \to R, \cancel{P} \vdash R$ $\Rightarrow$ mp

$\vdash (P \to Q) \to (Q \to R) \to P \to R$ $\Rightarrow$ abs : introduction d'implication

$P \to Q \to R, Q, P \vdash P \to Q \to R$ var $\quad P \to Q \to R, Q, P \vdash P$ var

$P \to Q \to R, Q, P \vdash Q \to R$ $\Rightarrow$ mp $\quad P \to Q \to R, Q, P \vdash Q$ $\Rightarrow$ var

$P \to Q \to R, Q, P \vdash R$ $\Rightarrow$ mp

$P \to Q \to R \vdash Q \to P \to R$ $\Rightarrow$ i

$\vdash (P \to Q \to R) \to (Q \to P \to R)$ $\Rightarrow$ i

$A \wedge B$ conjonction

$A \vee B$ disjonction

TD 7 : Calcul des séquents

exercice 7.3 :

ax

$A \vdash A$

aff$_g$

$A, B \vdash A$

$\rightarrow_d$

$A \vdash B \rightarrow A$

$\rightarrow_d$

$\vdash A \rightarrow (B \rightarrow A)$

Π : $A, (A \rightarrow B), (B \rightarrow C) \vdash C$

$\rightarrow_g$

$A, (A \rightarrow B) \vdash C, B$ $\quad\quad$ $A, (A \rightarrow B), C \vdash C$

aff$_d$ $\quad\quad$ aff$_g^*$

$A, (A \rightarrow B) \vdash B$ $\quad\quad$ $C \vdash C$

$\rightarrow_g$ $\quad\quad$ ax

$A \vdash B, A$ $\quad\quad$ $A, B \vdash B$

aff$_d$ $\quad\quad$ aff$_g$

$A \vdash A$ $\quad\quad$ $B \vdash B$

ax $\quad\quad$ ax

$\vdash (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow A \rightarrow C))$

$\rightarrow_d^*$

$(A \rightarrow (B \rightarrow C)), A \rightarrow B, A \vdash C$

$\rightarrow_g$

$A \rightarrow B, A \vdash A, C$ $\quad\quad$ $A \rightarrow B, A, B \rightarrow C \vdash C$

aff$_g$+aff$_d$+ax $\quad\quad$ Π

$\vdash ((P \rightarrow Q) \rightarrow P) \rightarrow P$

$\rightarrow_d$

$(P \rightarrow Q) \rightarrow P \vdash P$

$\rightarrow_g$

$\vdash P, P \rightarrow Q$ $\quad\quad$ $P \vdash P$

$\rightarrow_d$ $\quad\quad$ ax

$P \vdash P, Q$

aff$_d$ + ax

exercice 7.4

$\neg \exists x\, R(x) \vdash \forall x\, \neg R(x)$

$\forall_d$ $\quad$ car $x \notin VL(\neg \exists x\, R(x))$

$\neg \exists x\, R(x) \vdash \neg R(x)$

$\neg_d$

$\neg \exists x\, R(x), R(x) \vdash$

$\neg_g$

$R(x) \vdash \exists x\, R(x)$

$\exists_d$

$R(x) \vdash R(x)$

ax

$\neg \forall x\, R(x) \vdash \exists x\, \neg R(x)$

——— $\neg g$

$\vdash \exists x\, \neg R(x), \forall x\, R(x)$

——— $\forall d$

$\vdash \exists x\, \neg R(x), R(x)$

——— $\exists d$

$\vdash \neg R(x), R(x)$

——— $\neg d$

$R(x) \vdash R(x)$

——— ax

$\vdash \forall x\, (Q \vee R(x)) \rightarrow Q \vee \forall x\, R(x)$

——— $\rightarrow d$

$\forall x\, (Q \vee R(x)) \vdash Q \vee \forall x\, R(x)$

——— $\vee d$

$\forall x\, (Q \vee R(x)) \vdash Q, \forall x\, R(x)$

——— $\forall g$

$Q \vee R(x) \vdash Q, \forall x\, R(x)$

——— $\vee g$

$R(x) \vdash Q, \forall x\, R(x)$ $\qquad$ $Q \vdash Q, \forall x\, R(x)$

——— $\forall d$ $\qquad$ ——— aff d + ax

$R(x) \vdash Q, R(x)$

——— aff d + ax

$\vdash \exists x\, \forall y\, (R(y) \rightarrow R(x))$

——— contr

$\vdash \exists y\, \forall x\, (R(x) \rightarrow R(y)), \exists x\, (\forall z\, R(z) \rightarrow R(x))$

——— $\exists d$

$\vdash \forall x\, (R(x) \rightarrow R(y)), \exists x\, \forall z\, (R(z) \rightarrow R(x))$

——— $\forall d$ $\quad x \notin VL$

$\vdash (R(x) \rightarrow R(y)), \exists x\, \forall z\, (R(z) \rightarrow R(x))$

——— $\exists d$

$\vdash R(x) \rightarrow R(y), \forall z\, (R(z) \rightarrow R(x))$

——— $\forall d$ $\quad z \notin VL$

$\vdash R(x) \rightarrow R(y), R(z) \rightarrow R(x)$

——— $\rightarrow d$

$R(x), R(z) \vdash R(y), R(x)$

——— aff g+d

$R(x) \vdash R(x)$

——— ax.

exercice 7.5:

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

——— $\wedge d$

$\neg (A \vee B) \vdash \neg A$ $\qquad$ $\neg (A \vee B) \vdash \neg B$

——— $\neg d$ $\qquad$ ——— $\neg d$

$\neg (A \vee B), A \vdash$ $\qquad$ $\neg (A \vee B), B \vdash$

——— $\neg g$ $\qquad$ ——— $\neg g$

$A \vdash A \vee B$ $\qquad$ $B \vdash A \vee B$

——— $\vee_d^1$ $\qquad$ ——— $\vee_d^2$

$A \vdash A$ $\qquad$ $B \vdash B$

——— ax $\qquad$ ——— ax

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

$\overline{\neg A, \neg B \vdash \neg(A \vee B)}$ $\wedge g$

$\overline{\neg A, \neg B, A \vee B \vdash}$ $\neg d$

$\overline{A \vee B \vdash A, B}$ $\neg g$

$\overline{A \vdash A, B \qquad B \vdash A, B}$ $\vee g$

$\overline{A \vdash A}$ aff d $\qquad \overline{B \vdash B}$ aff d

$\overline{}$ ax $\qquad \overline{}$ ax

$A \vdash \neg\neg A$

$\overline{A, \neg A \vdash}$ $\neg d$

$\overline{A \vdash A}$ $\neg g$

$\overline{}$ ax

$\neg\neg\neg A \vdash \neg A$

$\overline{\neg\neg\neg A, A \vdash}$ $\neg d$

$\overline{A \vdash \neg\neg A}$ $\neg g$

$\overline{}$ ax

exercice 7.6

$\forall x \neg R(x) \vdash \neg \exists x R(x)$

$\overline{\forall x \neg R(x), \exists x R(x) \vdash}$ $\neg d$

$\overline{\forall x \neg R(x), R(x) \vdash}$ $\exists g$ $\quad x \notin VL$

$\overline{\neg R(x), R(x) \vdash}$ $\forall g$

$\overline{R(x) \vdash R(x)}$ $\neg g$

$\overline{}$ ax.

exercice 7.1 :

$\dfrac{\Gamma \vdash \Delta}{\Gamma' \vdash \Delta'}\, n \rightsquigarrow \dfrac{D(\Delta) \vdash D(\Gamma)}{D(\Delta') \vdash D(\Gamma')}\, n'$

$\dfrac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \qquad \dfrac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\, \vee d$ $\quad$ réversible ?

$\rightarrow g$ est-elle réversible ?

$\rightarrow d$ est elle réversible ?

$$\frac{\Gamma \vdash A \vee B, \Delta}{\Gamma \vdash A, B, \Delta} \quad \text{(règle dérivée)}$$

en utilisant la coupure.

$$\begin{array}{c}
\Gamma \vdash A, B, \Delta \\
\hline
\Gamma \vdash A \vee B, \Delta \qquad A \vee B \vdash A, B
\end{array} \; \text{coupure}$$

$$\begin{array}{cc}
\multicolumn{2}{c}{A \vee B \vdash A, B} \\
\hline
A \vdash A, B & B \vdash A, B \\
\hline
A \vdash A & B \vdash B \\
\hline
\text{ax} & \text{ax}
\end{array} \quad (\vee_g,\ \text{aff},\ \text{aff})$$

$$\begin{array}{c}
\Gamma, A \to B \vdash \Delta \\
\hline
\Gamma \vdash A, \Delta \qquad \Gamma, B \vdash \Delta
\end{array} \; \to_g$$

$$\begin{array}{c}
\Gamma, A \to B \vdash \Delta \\
\hline\hline
\Gamma \vdash A, \Delta
\end{array} \; ? \quad \text{oui} \qquad ? \; \begin{array}{c}
\Gamma, A \to B \vdash \Delta \\
\hline\hline
\Gamma, B \vdash \Delta
\end{array}$$

$\mathcal{M} \models \Gamma$ cas 1 : $\mathcal{M} \models A \to B$ donc par hypothèse $\mathcal{M} \models \Delta$

cas 2 : $\mathcal{M} \not\models A \to B$ donc $\mathcal{M} \models \neg(A \to B)$ donc $\mathcal{M} \models A, \Delta$

$$\begin{array}{l}
\Gamma \vdash A, \Delta \\
\hline
\Gamma, \Gamma \vdash A, \Delta \quad \text{contr } g \\
\hline
\Gamma \vdash A, A \to B \qquad \Gamma, A \to B \vdash \Delta \quad \text{coupure} \\
\hline
\Gamma, A \vdash A, B \quad \to d \\
\hline
\text{aff } g+d + \text{ax}
\end{array}$$

$\mathcal{M} \models (\Gamma, A \to B \vdash \Delta)$

si $\mathcal{M} \models \Gamma \wedge B$ alors $\mathcal{M} \models \Gamma \wedge (A \to B)$ donc $\mathcal{M} \models \Delta$.

$$\begin{array}{l}
\Gamma, B \vdash \Delta \\
\hline
\Gamma, B \vdash \Delta, \Delta \quad \text{contr } d \\
\hline
B \vdash \Delta, A \to B \qquad \Gamma, A \to B \vdash \Delta \quad \text{coup} \\
\hline
B, A \vdash \Delta, B \quad \to d \\
\hline
\text{aff } g+d + \text{ax}.
\end{array}$$

Exercice 7.2

$F \vDash\!\dashv G \qquad F \vDash G$ et $G \vDash F$

$\forall \mathcal{A}$ structure sur $(\mathcal{F}, \mathcal{R})$, $\forall v$ valuation,

$(\mathcal{A}, v) \vDash F$ alors $(\mathcal{A}, v) \vDash G$

$\forall \mathcal{A}$ structure sur $(\mathcal{F}, \mathcal{R})$, $\forall v$ valuation,

$(\mathcal{A}, v) \vDash F(\neg A_1, \dots, \neg A_m) \Leftrightarrow (\mathcal{A}, v) \vDash \neg D(F)(A_1, \dots, A_m)$.

Par récurrence sur $|F|$ (F est vue comme un mot)

* $F = \bot$: $D(F) = \top$

$$\underbrace{(\mathcal{A}, v) \vDash \bot}_{\text{faux}} \Leftrightarrow \underbrace{(\mathcal{A}, v) \vDash \neg \top}_{\text{faux.}}$$

* $F = A_1$ formule atomique

$R_i(t_1, t_2, \dots, t_k)$ $k = ar(R_i)$ t_i termes

$D(F) = F$

$(\mathcal{A}, v) \vDash F(\neg A_1) \Leftrightarrow (\mathcal{A}, v) \vDash \neg A_1 \Leftrightarrow (\mathcal{A}, v) \vDash \neg D(F)$

* $F = \top \qquad D(F) = \bot$

$(\mathcal{A}, v) \vDash \top \Leftrightarrow (\mathcal{A}, v) \vDash \neg \bot$

* $F = G \wedge H$

$G \wedge H[\neg A_i / A_i] \overset{?}{\vDash\!\dashv} \neg D(G \wedge H)$

$G[\neg A_i / A_i] \wedge H[\neg A_i \backslash A_i]$

par hypothèse d'induction,

$G[\neg A_i / A_i] \vDash\!\dashv \neg D(G)$

$H[\neg A_i / A_i] \vDash\!\dashv \neg D(H)$

$$\begin{aligned} G[\neg A_i / A_i] \wedge H[\neg A_i / A_i] &\vDash\!\dashv \neg D(G) \wedge \neg D(H) \\ &\vDash\!\dashv \neg (D(G) \vee D(H)) \\ &= \neg D(G \wedge H) = \neg D(F) \end{aligned}$$

* $F = G \to H$

$$\begin{aligned} G[\neg A_i / A_i] \to H[\neg A_i / A_i] &\vDash\!\dashv \neg D(G) \to \neg D(H) \\ &\vDash\!\dashv D(H) \to D(G) \\ &\vDash\!\dashv \neg\neg (D(H) \to D(G)) \end{aligned}$$

$\models\!\dashv \neg (D(G \to H))$

2. $(\mathcal{C}, v) \models S = F_1, \dots, F_m \vdash G_1, \dots, G_m$

$(\mathcal{C}, v) \models F_1 \wedge \dots \wedge F_m \to G_1 \vee \dots \vee G_m$

la question 1 montre que

si $(\mathcal{C}, v) \models F[A_i / A_i]$ mais aussi pour $(\mathcal{C}', v')$ au lieu de $(\mathcal{C}, v)$

alors $(\mathcal{C}, v) \models \neg D(F)$

$$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \rightsquigarrow D$$

$$\frac{D(\Delta) \vdash D(\Gamma), D(A), D(B)}{D(\Delta) \vdash \{D(\Gamma), D(A) \vee D(B)} \vee d$$ règle duale de $\wedge d$

$\vee_g \rightsquigarrow \wedge d$

$\neg_g \rightsquigarrow \neg d$

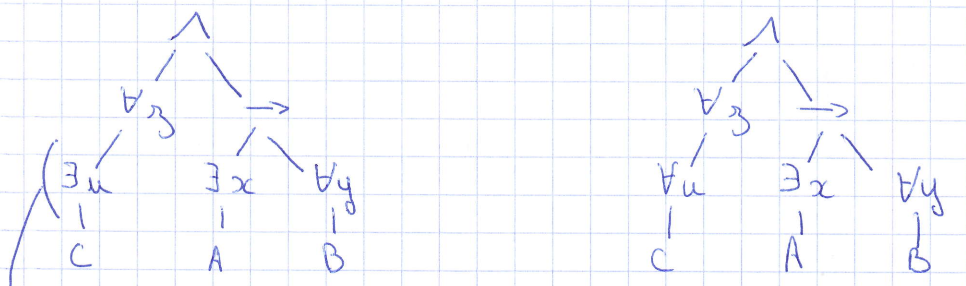
coupure $\rightsquigarrow$ coupure.

Exercice 8.1

TH : Si $\Gamma \vdash \exists x\, A$ est prouvable dans LJ et si Γ ne contient que des formules "de Harrop" alors il existe un terme t tel que $\Gamma \vdash_{LJ} A[x := t]$

ϕ est une formule de Harrop si elle ne contient pas de symbole $\exists$ ni de symbole $\vee$ dans un contexte strictement positif.

$A \to B \equiv_{LK} \neg A \vee B$ ⚠ faux dans LJ



: formule de Harrop.

> pas de Harrop parce qu'on est dans un contexte positif

COMPF :

f : symbole de fonction d'arité $k = 2$

$\forall x_1, x_2, y_1, y_2, (x_1 = y_1 \wedge x_2 = y_2) \to (f(x_1, x_2) = f(y_1, y_2))$

EG : th. de Harrop.

$PO = PO - \{A2\}$

Pour chaque formule ϕ, REC_ϕ est un axiome.

Certaines instances de REC_ϕ ne sont pas de Harrop.

exemple : $H(x) : x = 0 \vee \exists y \; x = S(y)$

REC_H n'est pas de Harrop.

MO : th. de Harrop

GR : théorie de Harrop

Exercice 8.2

1. PO' est une théorie de Harrop (resp. PA')
2. $PA' \vdash_{LK} A2$

$$\forall x \; \underbrace{x = 0 \vee \exists y, x = S(y)}_{H(x)}$$

$\mathcal{S} = \langle \mathcal{F}, \mathcal{R} \rangle$

$\mathcal{F} = \{S, +, \times\}$ $\mathcal{R} = \{=\}$

à partir de Ea

$H(0) : 0 = 0 \vee \exists y, 0 = S(y)$ introduction de $\vee$ à droite

$H(x) \to H(x+1)$

membre gauche du séquent

hypothèse : $x = 0 \vee \exists y, x = S(y)$

$S(x) = S(x)$

donc $\exists y, S(x) = S(y)$

donc $S(x) = 0 \vee \exists y, S(x) = S(y)$ $\forall x \; H(x) \to H(x+1)$ introduire $\to$ à droite

$H(0) \wedge \forall x \; H(x) \to H(x+1)$ introduire $\wedge$ à droite

Par récurrence sur x, on a prouvé $\forall x, H(x)$

$PA' \vdash 0 = 0 \vee \exists y \; 0 = S(y)$ $\quad \Pi 0$

$PA' \vdash H(0) \wedge \forall x \; H(x) \to H(x+1)$ $\Pi 1$

$$\cfrac{\cfrac{\cfrac{\cfrac{\overline{x = x[x := 0] \vdash 0 = 0}\;\text{ax}}{\forall x, x = x \vdash 0 = 0}\;\forall g}{PA' \vdash 0 = 0, \exists y \; 0 = S(y)}\;\text{aff}_{d+g}}{PA' \vdash 0 = 0 \vee \exists y, 0 = S(y)}\;\vee d}{}$$

$$\dfrac{\dfrac{}{PA' \vdash H0}\,\Pi 0 \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{x = x\,[x := S(x)] \vdash S(x) = S(x)}\,ax}{\forall x\; x = x \vdash S(x) = S(x)}\,\forall g}{PA', H(x) \vdash S(x) = S(y)\,[y := x]}\,aff_g}{PA', H(x) \vdash \exists y\; S(x) = S(y)}\,\exists d}{PA', H(x) \vdash S(x) = 0,\; \exists y\, S(x) = S(y)}\,aff_d}{PA', H(x) \vdash S(x) = 0 \vee \exists y\; S(x) = S(y)}\,\vee d}{PA', H(x) \vdash \forall x\,(S(x) = 0 \vee \exists y\; S(x) = S(y))}\,\forall d}{PA' \vdash H(x) \to H(S(x))}\,\to x}{PA' \vdash \forall x\; H(x) \to H(S(x))}\,\forall d}{PA' \vdash H0 \wedge \forall x\; H(x) \to H(S(x))}\,\wedge d$$

$PA'_H = EG_\varphi + P0' + REC_H$

Exercice 8.3

P_0' : A1, A3, A4, A5, A6, A7

$REC_H \wedge A_1 \wedge A_3 \dots \wedge A_7 \vdash_{LK} A_2$

$Q : \overset{EG\wedge}{A_1} \wedge A_3 \wedge A_4 \wedge A_5 \wedge A_6 \wedge A_7 \vdash_{LK} A_2$?

Interpréter la signature

$S \longrightarrow S_{\mathcal{P}}$ $\qquad + \longrightarrow +_{\mathcal{P}}$

$0 \longrightarrow 0_{\mathcal{P}}$ $\qquad \times \longrightarrow \times_{\mathcal{P}}$

$= \longrightarrow =$

EG : $=_{\mathcal{P}}$ est l'égalité $\to$ EG est vérifié $\qquad 0_{\mathcal{P}} = \langle 0, \circ \rangle$

A_1: $\forall x \in \mathcal{P},\ \neg S_{\mathcal{P}}(x) = \langle 0, \circ \rangle$

$S_{\mathcal{P}}(p, \alpha) = \langle p+1, \alpha \rangle \neq \langle 0, \circ \rangle$ $\qquad$ A_1 est vérifié

A_3: $\forall x, y\ \ S(x) = S(y) \to x = y$

$S_{\mathcal{P}} \langle p, \alpha \rangle = S_{\mathcal{P}} \langle q, \beta \rangle \overset{?}{\to} \langle p, \alpha \rangle = \langle q, \beta \rangle$

$S_{\mathcal{P}} \langle p, \alpha \rangle = S_{\mathcal{P}} \langle q, \beta \rangle \Leftrightarrow \langle p+1, \alpha \rangle = \langle q+1, \beta \rangle$

$\Leftrightarrow \begin{cases} p+1 = q+1 \\ \alpha = \beta \end{cases} \Leftrightarrow \begin{cases} p = q \\ \alpha = \beta \end{cases} \Rightarrow \langle p, \alpha \rangle = \langle q, \beta \rangle$

$\langle p, \alpha \rangle +_{cp} \langle q, \beta \rangle = \langle p+q, \alpha \rangle$

$\langle p, \alpha \rangle \times_{cp} \langle q, \beta \rangle = \langle p \times q, \beta \rangle$

$A_4 : \langle p, \alpha \rangle +_{cp} \langle 0, \cdot \rangle = \langle p+0, \alpha \rangle = \langle p, \alpha \rangle$ OK

$A_5 : \langle p, \alpha \rangle +_{cp} S_{cp} \langle q, \beta \rangle = \langle p, \alpha \rangle +_{cp} \langle Sq, \beta \rangle = \langle p+q+1, \alpha \rangle$

$S_{cp}(\langle x, \alpha_1 \rangle +_{cp} \langle y, \beta_1 \rangle) = S_{cp} \langle x+y, \alpha_1 \rangle = \langle x+y+1, \alpha \rangle$

$A_6 : \langle p, \alpha \rangle \times_{cp} \langle 0, \cdot \rangle = \langle p \times 0, \beta \rangle = \langle 0, \beta \rangle$ OK

$A_7 : \langle p, \alpha \rangle \times_{cp} S_{cp} \langle q, \beta \rangle = \langle p, \alpha \rangle \times_{cp} \langle q+1, \beta \rangle$

$= \langle p \times (q+1), \beta \rangle$

$= \langle p \times q + p, \beta \rangle$

$\langle p, \alpha \rangle \times_{cp} \langle q, \beta \rangle +_{cp} \langle p, \gamma \rangle = \langle p \times q, \beta \rangle +_{cp} \langle p, \gamma \rangle$

$= \langle p \times q + p, \beta \rangle$ OK

On a montré $\mathcal{A} \models A_1 \wedge A_3 \wedge A_4 \wedge A_5 \wedge A_6 \wedge A_7$

$A_2 : \forall x \, (x = 0 \vee \exists y, x = S(y))$

Pour $\langle 0, 0 \rangle$

on a $\langle 0, 0 \rangle \neq 0_{cp}$

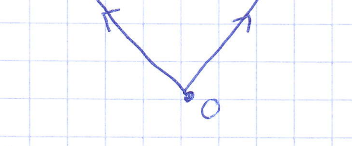
on suppose (absurde)

$\exists \langle q, \alpha \rangle, \langle 0, 0 \rangle = S(\langle q, \alpha \rangle) \rightarrow 0 = S(q)$ contredit A_1 dans $\mathbb{N}$

Donc $A_1 \wedge A_3 \wedge A_4 \wedge A_5 \wedge A_6 \wedge A_7 \vdash A_2$ n'est pas prouvable dans LK

Exercice 9.2

Dans LK : $\vdash \overbrace{\overbrace{(\underbrace{\neg A}_{F_1} \rightarrow B)}^{F_3} \rightarrow \overbrace{(\underbrace{\neg B}_{F_2} \rightarrow A)}^{F_4}}^{F}$



$1 \Vdash A$ $\quad 0 \nVdash A$

$2 \Vdash B$ $\quad 0 \nVdash B$

$1 \nVdash \neg A$ $\quad 0 \nVdash \neg B$

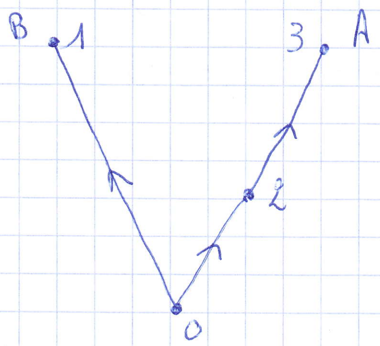
$0 \nVdash \neg A$ (argument de croissance)

$1 \Vdash \neg A \rightarrow B$ $\quad 0 \Vdash \neg A \rightarrow B$ $\quad (\forall k \geq 0$, si $k \Vdash \neg A$ alors $k \Vdash B)$

$2 \Vdash \neg A \rightarrow B$ $\quad$ symétriquement : $0 \Vdash \neg B \rightarrow A$

$1 \Vdash \neg B \to A$

donc $0 \Vdash (\neg A \to B) \to (\neg B \to A)$



$1 \Vdash \neg A$ $\quad$ $3 \Vdash A$

$2 \nVdash A \to \bot$ $\quad$ $2 \nVdash \neg A$

$0 \nVdash \neg A$

$3 \Vdash \neg B$

$2 \Vdash \neg B$

$0 \nVdash \neg B$

$0 \Vdash \neg A \to B$ (R1)

en 1 : $1 \Vdash \neg A$, $1 \Vdash B$

en 0 : $0 \nVdash \neg A$

en 2 : $2 \nVdash \neg A$

en 3 : $3 \nVdash \neg A$

en 1 : $1 \nVdash \neg B$ car $1 \Vdash B$

en 0 : $0 \nVdash \neg B$

en 2 : $2 \Vdash \neg B$, $2 \nVdash A$

$0 \nVdash \neg B \to A$ (R2)

(R1)(R2) $\Rightarrow 0 \nVdash (\neg A \to B) \to (\neg B \to A)$

Donc le séquent n'est pas prouvable dans LJ.

$\vdash (A \to (B \to C)) \to ((A \to B) \to (A \to C))$

$\overline{}\ \to d^*$

$A \to (B \to C),\ A \to B,\ A \vdash C$

$\overline{}\ \to g$

$A \to B,\ A \vdash A \qquad B \to C,\ A \to B,\ A \vdash C$

$\overline{}\ \text{aff+ax} \qquad \overline{}\ \to g$

$A \to B, A \vdash B \qquad C, A \to B, A \vdash C$

$\overline{}\ \to g \qquad \overline{}\ \text{aff+ax}$

$A \vdash A \qquad B, A \vdash B$

$\overline{}\ \text{ax} \qquad \overline{}\ \text{aff+ax}$

Considérons la structure de Kripke $\mathcal{K} := (K, \leqslant, \Vdash)$ où

$K := \{0, 1, 2\}$, $\leqslant := \{(0,2), (0,1)\}$ et $\Vdash := \{(1,P), (2,Q)\}$

Par définition : $1 \Vdash P$ et $1 \nVdash Q$

Donc $1 \nVdash P \to Q$

Et comme $0 \leqslant 1$ on en déduit que : $0 \nVdash P \to Q$ (1)

En échangeant 1 avec 2 et P avec Q dans l'argument précédent, on obtient : $O \not\Vdash Q \rightarrow P$ (2)

Et de (1) et (2) on déduit que $O \not\Vdash (P \rightarrow Q) \vee (Q \rightarrow P)$

La structure $\mathcal{K}$ est un contre modèle de $(P \rightarrow Q) \vee (Q \rightarrow P)$.

Le séquent $\vdash (P \rightarrow Q) \vee (Q \rightarrow P)$ n'est donc pas prouvable dans LJ.

Université Bordeaux 1
Mastère d'Informatique 1, 2008/2009

LOGIQUE

Sujet de contrôle continu- 27 Novembre 2008

Durée : 2 H
Documents autorisés : notes de cours, feuilles et notes de TD.

Exercice 1(sur 4 points)
On se demande si certaines règles commodes pourraient être ajoutées à LK, sans modification de l' ensemble des séquents prouvables.
1- La règle suivante est-elle une règle dérivée du système LK ?

$$\frac{\Gamma \vdash A \quad \Gamma \vdash A \to B}{\Gamma \vdash B}$$

2- La règle suivante est-elle une règle dérivée du système LK ?

$$\frac{\Gamma \vdash \Delta, A, B \quad A, B, \Gamma' \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

Aide : on examinera soigneusement le cas d' une instantiation telle que $B = \neg A$.
3- Pour chacune de ces règles, dire si on peut la simuler par une dérivation sans coupure de LK.

Exercice 2(sur 4 points)
On se demande quelles propriétés algébriques possède l'implication. On considère les deux séquents S_1, S_2 suivants :

$$\begin{aligned} S_1 &:= (A \to B) \to C \vdash A \to (B \to C) \\ S_2 &:= (A \to B) \to C \vdash (A \to C) \to (B \to C) \end{aligned}$$

Pour chacun de ces deux séquents, déterminer s' il est prouvable dans LK ;
- si oui, donner une preuve dans LK,
- si non, donner un argument qui montre la non-existence d'une preuve.

Exercice 3(sur 6 points)
Donner des preuves dans LJ des séquents suivants :

$$\forall y \neg R(y) \vdash \forall y (R(y) \to R(x))$$

$$\neg \exists x R(x) \vdash \forall x \neg R(x))$$

$$\neg \exists x R(x) \vdash \exists x \forall y (R(y) \to R(x))$$

Exercice 4(sur 6 points)
Une dérivation est dite *atomique* si tout axiome $A \vdash A$ y figurant est de la forme $\bot \vdash \bot$ ou $P \vdash P$, où P est une proposition atomique (par opposition à une formule comportant au moins un connecteur ou un quantificateur). Montrer que pour toute formule A, le séquent $A \vdash A$ admet une dérivation atomique dans LJ.