

## LOGIQUE, INF 462

Examen du 20/12/2010-Sujet de M. Sénizergues ;

Le barème est réévalué comme suit :

Ex 4 : 4 pts ; Ex 5 : 3 pts ; Ex 6 : 14 pts. La note obtenue sur cette partie est le minimum entre 10 et le total obtenu sur les exercices 4,5,6.

### Exercice 4

Les règles R1,R2 sont des règles dérivées du système LK :

$$\begin{array}{c}
 \frac{\frac{\frac{\frac{}{B \vdash B, C}{}^{\text{ax}'}}{B, C \vdash C}{}^{\text{ax}'}}{B \rightarrow C, B \vdash C}{}^{\rightarrow_g}}{B \rightarrow C, A \vdash A, C}{}^{\text{ax}'}}{B \rightarrow C, A, B \vdash C}{}^{\text{aff}_g}}{A \rightarrow B, B \rightarrow C, A \vdash C}{}^{\rightarrow_g}}{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash B \rightarrow C \quad \frac{A \rightarrow B, B \rightarrow C \vdash A \rightarrow C}{}^{\rightarrow_d}}{\Gamma \vdash (A \rightarrow B) \wedge (B \rightarrow C)}{}^{\wedge_d} \quad \frac{A \rightarrow B, B \rightarrow C \vdash A \rightarrow C}{}^{\rightarrow_d}}{(A \rightarrow B) \wedge (B \rightarrow C) \vdash A \rightarrow C}{}^{\wedge_g} \quad \frac{\Gamma \vdash B \quad B \vdash \Delta}{}{\Gamma \vdash \Delta}{}_{\text{coupure}}}{\Gamma \vdash A \rightarrow C}{}_{\text{coupure}}
 \end{array}$$

Considérons le système étendu LK + R3. Ce système étendu admet la preuve suivante du séquent vide :

$$\frac{\frac{\frac{}{B \vdash B}{}^{\text{ax}}}{\vdash B, \neg B}{}^{\neg_d} \quad \frac{\frac{}{B \vdash B}{}^{\text{ax}}}{B, \neg B \vdash}{}^{\neg_g}}{\vdash}{}_{R3}$$

Comme  $\vdash$  n'est pas prouvable dans LK, les systèmes (LK + R3) et LK ne sont pas équivalents, ce qui entraîne que R3 n'est pas une règle dérivée du système LK.

La règle R4 est une règle dérivée du système LK :

$$\frac{\frac{\frac{\frac{\frac{}{A \vdash A, B}{}^{\text{ax}'}}{A, B \vdash B}{}^{\text{ax}'}}{A \rightarrow B, A \vdash B}{}^{\rightarrow_g} \quad \frac{\frac{\frac{\frac{}{A \vdash A, C}{}^{\text{ax}'}}{A, C \vdash C}{}^{\text{ax}'}}{A \rightarrow C, A \vdash C}{}^{\rightarrow_g}}{A \rightarrow B, A \vdash B, C}{}^{\text{aff}_d} \quad \frac{\frac{\frac{\frac{}{A \vdash A, C}{}^{\text{ax}'}}{A, C \vdash C}{}^{\text{ax}'}}{A \rightarrow C, A \vdash C}{}^{\rightarrow_g}}{A \rightarrow C, A \vdash B, C}{}^{\text{aff}_d}}{A \rightarrow B, A \vdash B \vee C}{}^{\vee_d} \quad \frac{\frac{\frac{\frac{}{A \vdash A, C}{}^{\text{ax}'}}{A, C \vdash C}{}^{\text{ax}'}}{A \rightarrow C, A \vdash C}{}^{\rightarrow_g}}{A \rightarrow C, A \vdash B \vee C}{}^{\vee_d}}{A \rightarrow B \vdash A \rightarrow (B \vee C)}{}^{\rightarrow_d} \quad \frac{\frac{\frac{\frac{}{A \vdash A, C}{}^{\text{ax}'}}{A, C \vdash C}{}^{\text{ax}'}}{A \rightarrow C, A \vdash C}{}^{\rightarrow_g}}{A \rightarrow C \vdash A \rightarrow (B \vee C)}{}^{\rightarrow_d}}{(A \rightarrow B) \vee (A \rightarrow C) \vdash A \rightarrow (B \vee C)}{}^{\vee_g}}{\Gamma \vdash (A \rightarrow B) \vee (A \rightarrow C)}{}_{\text{coupure}}}{\Gamma \vdash A \rightarrow (B \vee C)}{}_{\text{coupure}}$$

### Exercice 5

Le séquent  $S_1$  est réfuté par la structure de Kripke suivante :

$$\mathcal{K}_1 := \langle K, \leq, \Vdash \rangle$$

où  $K = \{0, 1\}$ ,  $\leq = \{(0, 0), (1, 1), (0, 1)\}$ ,  $\Vdash_0 = \{(1, A), (1, B)\}$  (voir la figure 1).

En effet, le noeud 0 vérifie :

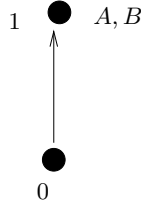


FIG. 1 –  $\mathcal{K}_1$ .

$\forall k' \geq 0$ , si  $k' \Vdash A$  alors  $k' \Vdash B$

donc

$$0 \Vdash A \rightarrow B. \quad (1)$$

D'autre part, comme  $0 \leq 1$  (pour l'ordre sur les noeuds de  $\mathcal{K}_1$ ), et  $1 \Vdash A$

$$0 \not\Vdash \neg A$$

et comme, par définition de la relation de forçage  $\Vdash_0$ ,  $0 \not\Vdash B$ , on a

$$0 \not\Vdash \neg A \vee B \quad (2)$$

Les relations (1) et (2) montrent que le séquent

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

n'est pas valide dans  $\mathcal{K}_1$ . Ce séquent n'est donc pas prouvable dans LJ.

$S_2$  admet la preuve suivante (dans LJ) :

$$\frac{\frac{\frac{\overline{A \vdash A}^{\text{ax}}}{\neg A, A \vdash}^{\neg_g}}{\neg A, A \vdash B}^{\text{aff}_d} \quad \frac{\overline{B, A \vdash B}^{\text{ax}'}}{\neg A \vee B, A \vdash B}^{\vee_g}}{\neg A \vee B \vdash A \rightarrow B}^{\rightarrow_d}$$

### Exercice 6

1-

$$S(u, w) = (a, a)(b, b)(b, a)(\#, b); \quad S(v, w) = (b, a)(a, b)(a, a)(b, b)(a, \#).$$

2- Les trois langages  $L_=, L_{\approx}, L_{\preceq}$  sont décrits par les expressions rationnelles suivantes :

$$L_= = \{(x, x) \mid x \in X\}^*; \quad L_{\approx} = \{(x, y) \mid x \in X, y \in X\}^*; \quad L_{\preceq} = \{(x, x) \mid x \in X\}^* \cdot \{(\#, x) \mid x \in X\}^*.$$

3- Soit  $x \in X$ . Le langage  $L_x$  est décrit par l'expression rationnelle :

$$L_x = L_= \cdot \{(\#, x)\}.$$

4- On procède comme pour la preuve du théorème de Büchi-Bruyère, vue en cours.

Remarquons que toute formule du premier ordre (sur le langage de l'énoncé) peut être transformée en une formule équivalente  $\Phi$ , dont toutes les sous-formules atomiques sont de l'une des quatre formes :

$$u \approx v, \quad u = v, \quad u \preceq v, \quad u \cdot x = v$$

(où  $x \in X$  et  $u, v$  sont des variables). Soit  $\Phi$  une telle formule et soient  $\{z_1, z_2, \dots, z_n\}$  un ensemble de variables qui contient toutes les variables de  $\Phi$ . Notons

$$L(\Phi, z_1, \dots, z_n) := \{S(u_1, u_2, \dots, u_n) \mid u_1, u_2, \dots, u_n \in X^*, \mathcal{M} \models \Phi(u_1, u_2, \dots, u_n)\}$$

On démontre par récurrence sur  $|\Phi| + n$  que  $L(\Phi, z_1, \dots, z_n)$  est rationnel.

**Base** :  $\Phi$  est atomique et  $n \leq 2$ .

Si  $n = 2$  : d'après la question 2,  $L(\Phi, z_1, z_2)$  est rationnel.

Si  $n = 1$  : alors  $z_1 = z_2$ . Dans ce cas,  $L(\Phi, z_1) = X^*$  ou  $L(\Phi, z_1) = \emptyset$ , donc  $L(\Phi, z_1)$  est rationnel.

**Cas 1**(ajout d'une variable) :  $z_1$  n'apparaît pas dans  $\Phi$ .

Par hypothèse de récurrence,  $L(\Phi, z_2, \dots, z_n)$  est rationnel. Soit  $\pi_{2,n} : ((X \cup \{\#\})^n)^* \rightarrow ((X \cup \{\#\})^{n-1})^*$  l'homomorphisme défini par

$$\pi_{2,n}(a_1, a_2, \dots, a_n) = (a_2, \dots, a_n).$$

Soit  $SUP_n \subseteq ((X \cup \{\#\})^n)^*$  l'ensemble des superpositions de  $n$  mots de  $X$ .

$$SUP_n = \{u \in ((X \cup \{\#\})^n)^* \mid \forall i \in [1, n], \pi_i(u) \in X^* \cdot \{\#\}^* \text{ et } \exists i \in [1, n], \pi_i(u) \in X^*\},$$

où  $\pi_i : ((X \cup \{\#\})^n)^* \rightarrow (X \cup \{\#\})^*$  est la projection sur la  $i$ -ième composante. Comme l'ensemble des langages rationnels est clos par homomorphisme inverse et par opérations booléennes,  $SUP_n$  est rationnel.

Or

$$L(\Phi, z_1, z_2, \dots, z_n) = \pi_{2,n}^{-1}(L(\Phi, z_2, \dots, z_n) \cdot (\#, \dots, \#)^*) \cap SUP_n.$$

Donc  $L(\Phi, z_1, z_2, \dots, z_n)$  est rationnel.

**Cas 2**(connecteur) :  $\Phi = \psi \circ \theta, n \geq 0$  où  $\circ$  est l'un des connecteurs  $\vee, \wedge, \neg$ .

$$L(\Phi, z_1, z_2, \dots, z_n) = L(\psi, z_1, z_2, \dots, z_n) \odot L(\theta, z_1, z_2, \dots, z_n)$$

où  $\odot$  est l'opérateur booléen qui traduit le connecteur  $\circ$  selon le dictionnaire :

$$(\vee, \wedge, \neg) \rightarrow (\cup, \cap, L \mapsto (SUP_n - L))$$

**Cas 3**(quantificateur existentiel) :  $\Phi = \exists z_1 \psi$ .

Posons

$$P := [\pi_{2,n}(L(\psi, z_1, z_2, \dots, z_n))].$$

Par hypothèse de récurrence  $P$  est rationnel.

Les mots de  $L(\Phi, z_1, z_2, \dots, z_n)$  sont les superpositions de  $n$  mots de  $X^*$  dont la projection sur les composantes  $2, 3, \dots, n$  (i.e. l'image par  $\pi_{2,n}$ ) est égale à celle d'un mot de  $L(\psi, z_1, z_2, \dots, z_n)$ , sauf pour un suffixe dans  $(\#, \#, \dots, \#)^*$ . Plus formellement :

$$L(\Phi, z_1, z_2, \dots, z_n) = [\pi_{2,n}^{-1}(P((\#, \dots, \#)^*)^{-1}) \cup \pi_{2,n}^{-1}(P(\#, \dots, \#)^*)] \cap SUP_n.$$

Les propriétés de stabilité de l'ensemble des langages rationnels par quotient à droite, par produit et par opérations booléennes entraînent que  $L(\Phi, z_1, z_2, \dots, z_n)$  est rationnel.

**Cas 4**(quantificateur universel) :  $\Phi = \forall z_1 \psi$ .

On remarque que  $\Phi$  est équivalente à

$$\Phi' := \neg \exists z_1 \neg \psi.$$

Par hypothèse de récurrence  $L(\psi, z_1, z_2, \dots, z_n)$  est rationnel. Par les transformations vues aux cas 2 et 3, il en résulte que  $L(\Phi, z_1, z_2, \dots, z_n)$  est rationnel.

5- Soit  $x \in X$ .

Considérons l'automate fini  $\mathcal{A}_x = \langle X, Q, D, Q_+, \delta \rangle$  tel que :  $Q := \{q_\varepsilon, q_\#\} \cup \{q_y \mid y \in X\}$ ,  $D := \{q_\varepsilon\}$ ,  $Q_+ := \{q_\#\}$  et  $\delta$  est l'ensemble de toutes les transitions de la forme :

$$\begin{aligned} q_\varepsilon &\xrightarrow{(y,x)} q_y \text{ où } y \in X \\ q_y &\xrightarrow{(z,y)} q_z \text{ où } y \in X, z \in X \\ q_y &\xrightarrow{(\#,y)} q_\# \text{ où } y \in X \\ q_\varepsilon &\xrightarrow{(\#,x)} q_\# \end{aligned}$$

Cet automate, lorsqu'il démarre dans l'état  $q_\varepsilon$  et lit un mot  $(y_0, x)(y_1, y_0) \cdots (y_i, y_{i-1}) \cdots (y_n, y_{n-1})$ , atteint l'état  $q_{y_n}$ ,

lorsqu'il lit  $(y_0, x)(y_1, y_0) \cdots (y_i, y_{i-1}) \cdots (y_n, y_{n-1})(\#, y_n)$ , atteint l'état  $q_\#$ ,

et ne peut lire, à partir de  $q_\varepsilon$ , que des mots de l'une de ces deux formes. Donc

$$L(\mathcal{A}_x) = \{S(u, v) \mid u, v \in X^*, x \cdot u = v\}.$$

6- Nous construisons une formule  $\Phi(u, v)$  qui exprime le fait que  $x \cdot u = v$ .

Cette formule  $\Phi$  est la conjonction de 4 formules *LONG*, *DEB*, *MIL*, *FIN* qui expriment, respectivement, que :

- $|u| + 1 = |v|$
- $v$  commence par la lettre  $x$
- si  $yz$  est un facteur de  $u$ , en position  $p$ , alors la lettre de  $v$ , en position  $p + 1$ , est aussi  $y$
- $u$  et  $v$  se terminent par une même lettre  $y$ .

Posons

$$LONG(u, v) := s_x(u) \approx v$$

$$DEB(u, v) := \forall w', [(\forall w, w' \preceq w) \rightarrow (s_x(w') \preceq v)]$$

$$MIL(u, v) := \forall w, \forall w', \bigwedge_{y \in X, z \in X} [(s_z(s_y(w)) \preceq u \wedge (s_z(s_y(w)) \approx w' \wedge w' \preceq v) \rightarrow (\exists w'', s_y(w'') = w'))]$$

$$FIN(u, v) := \forall w, \exists w', \bigwedge_{y \in X} [s_y(w) = u \rightarrow s_y(w') = v]$$

On définit alors

$$\Phi(u, v) := LONG(u, v) \wedge DEB(u, v) \wedge MIL(u, v) \wedge FIN(u, v).$$