Théorie de la démonstration

Examen final

27 avril 2011

Durée de l'épreuve : 3 heures.
Tous les documents sont autorisés.

Exercice 1. Donnez une preuve en **NK** (déduction naturelle classique) de la *loi de Pierce*, $((P \Rightarrow Q) \Rightarrow P) \Rightarrow P$.

Exercice 2. Soit $\mathbf{BT} = \forall X.X \Rightarrow (X \Rightarrow X \Rightarrow X) \Rightarrow X$ le type des arbres binaires dans le système **F**. Comme dans le cas des entiers, on peut démontrer que les termes normaux de type **BT** sont tous de la forme $\Lambda X.\lambda x^X f^{X\Rightarrow X\Rightarrow X}.T$, où T est un terme de type X engendré par la grammaire suivante :

$$T ::= x \mid fTT.$$

Trouvez un terme $G : \mathbf{BT} \Rightarrow \mathbf{BT}$ qui extrait le sous-arbre gauche, c'est-à-dire, tel que, pour tout $M : \mathbf{BT}$,

$$GM \to^* \begin{cases} M & \text{si } M \simeq_\beta \Lambda X.\lambda x^X f^{X\Rightarrow X\Rightarrow X}.x, \\ \Lambda X.\lambda x^X f^{X\Rightarrow X\Rightarrow X}.T_g & \text{si } M \simeq_\beta \Lambda X.\lambda x^X f^{X\Rightarrow X\Rightarrow X}.fT_gT_d. \end{cases}$$

Excercice 3. Dans la suite, on considère une interprétation fixée des formules de la logique linéaire multiplicative propositionnelle dans les espaces cohérents, c'est-à-dire, pour chaque formule A, on dispose d'un espace cohérent correspondant $[\![A]\!]$.

Soit π un réseau (la définition considérée ici est donnée en annexe). Une *expérience* sur π est une fonction e qui associe à chaque arête p de π étiquetée par A un element $e(p)$ de la trame de $[\![A]\!]$. Si les conclusions de π sont $\langle p_1, \ldots, p_n\rangle$, on définit le *résultat* de e, dénoté par $|e|$, comme la liste $\langle e(p_1), \ldots, e(p_n)\rangle$. De plus, on dit que l'expérience e est *positive* si les conditions suivantes sont satisfaites :

- pour tout lien ax (resp. cut) de π dont les conclusions (resp. premisses) sont p, q, on a $e(p) = e(q)$;
- pour tout lien $\otimes$ ou $⅋$ de π dont p, q, r sont respectivement la premisse gauche, la premisse droite et la conclusion, on a $e(r) = (e(p), e(q))$.

Donné un réseau π, on définit son *interprétation* $[\![\pi]\!]$ comme l'ensemble de tous les résultats des experiences positives sur π. Si π a conclusions typées par $A_1, \ldots, A_n$, $[\![\pi]\!]$ est donc un sous-ensemble de la trame de $[\![A_1]\!] ⅋ \cdots ⅋ [\![A_n]\!]$ (modulo le choix d'un parenthésage).

Démontrez la stabilité de l'interprétation par élimination des coupures, c'est-à-dire, que si π est un réseau tel que $\pi \to \pi'$, alors $[\![\pi]\!] = [\![\pi']\!]$. (*Suggestion : prouvez qu'il existe une expérience positive sur π si, et seulement si, il en existe une de même résultat sur π'*).

Exercice 4. Le système des *types avec intersection*, où *système* **I**, est un système de types « à la Curry » utilisant comme types les formules du fragment négatif (connecteurs $\Rightarrow$ et $\wedge$) de la logique minimale propositionnelle et défini par les règles de typage suivantes :

$$\frac{}{\Gamma, x : A \vdash x : A}$$

$$\frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x.M : A \Rightarrow B} \qquad \frac{\Gamma \vdash M : A \Rightarrow B \quad \Gamma \vdash N : A}{\Gamma \vdash MN : B}$$

$$\frac{\Gamma \vdash M : A \quad \Gamma \vdash M : B}{\Gamma \vdash M : A \wedge B} \qquad \frac{\Gamma \vdash M : A_1 \wedge A_2}{\Gamma \vdash M : A_i}\ i \in \{1, 2\}$$

où, comme d'habitude, Γ dénote un ensemble fini (éventuellement vide) d'assignations de types à des variables, de la forme $x : A$.

Soient $V = \lambda fu.fu$, $V' = \lambda vg.gv$, et $\Delta_3 = \lambda y.yyy$, et soit

$$U = (\lambda x.z(xV)(xV'))\Delta_3.$$

(a) Démontrez que U est fortement normalisable.

(b) Montrez que U est typable dans le système **I**. (*Suggestion : commencez par montrer que :*
- *V est typable de type $C = (X \Rightarrow Y) \Rightarrow X \Rightarrow Y$,*
- *V' est typable de type $C' = X \Rightarrow (X \Rightarrow Y) \Rightarrow Y$,*
- *Δ_3 est typable de type $E = ((X \Rightarrow Y \Rightarrow Z) \wedge X \wedge Y) \Rightarrow Z$,*

où X, Y, Z sont des atomes propositionnels, qui peuvent donc être remplacés par n'importe quelle autre formule plus complexe. En conséquence, on a que V est aussi typable avec $C_1 = C \Rightarrow C$ et $C_2 = C_1 \Rightarrow C \Rightarrow C$ (obtenus par le substitutions $C[X \Rightarrow Y/X, X \Rightarrow Y/Y]$ et $C[C/X, C/Y]$, respectivement). De façon similaire, si l'on pose $D = (C' \Rightarrow C') \Rightarrow C'$, on a que V' est aussi typable avec $C'_1 = C' \Rightarrow D$ et $C'_2 = C' \Rightarrow C'_1 \Rightarrow D$ (obtenus par le substitions $C'[C'/X, C'/Y]$ et $C'[C'/X, D/Y]$). Ensuite, remarquez que les types $F = (C_2 \wedge C_1 \wedge C) \Rightarrow C$ et $F' = (C'_2 \wedge C' \wedge C'_1) \Rightarrow D$ sont respectivement de la forme $E[C_1/X, C/Y, C/Z]$ et $E[C'/X, C'_1/Y, D/Z]$, et que Δ_3 et donc typable avec $F \wedge F'$... Dernière suggestion : le jugement de type à dériver sera

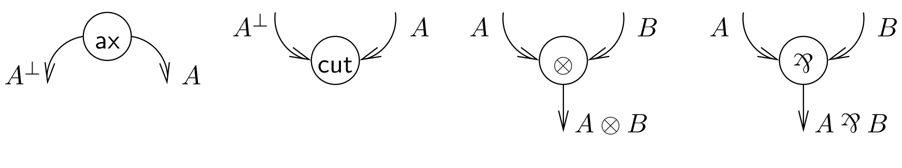
$$z : C \Rightarrow D \Rightarrow W \vdash U : W,$$

où W est n'importe quelle formule.).

(Le terme U est un exemple de terme fortement normalisable qui n'est pas typable dans le système **F**. Le système **I** donc type strictement plus de termes que le système **F** ; en fait, il est possible de démontrer qu'il type exactement les termes fortement normalisables).

Annexe : définition de réseau multiplicatif

Un *réseau* (ou *structure de preuve* dans la terminologie traditionnelle) est une structure graphique dirigée et étiquetée construite a partir des *liens* suivants :

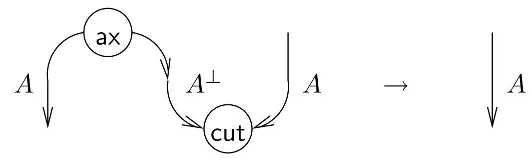


où les étiquettes A, B sont des formules de la logique linéaire multiplicative propositionnelle. Les arêtes entrantes (resp. sortantes) d'un lien sont appelées *premisses* (resp. *conclusions*) du lien. On demande qu'un réseau soit non vide et que chaque arête soit conclusion d'exactement un lien et premisse d'au plus un lien. Les arêtes d'un réseau qui ne sont premisses d'aucun lien sont appelées *conclusions* du réseau.

Les premisses des liens de type $\otimes$ et $⅋$ sont ordonnées, c'est-à-dire, on peut parler sans amibiguïté de *premisse gauche* et *premisse droite* d'un lien $\otimes$ ou $⅋$. Les conclusions d'un réseau sont elles aussi ordonnées, c'est-à-dire, elles forment une liste $\langle p_1, \ldots, p_n \rangle$, avec $n \in \mathbb{N}$.

On muni l'ensemble des réseaux de la réécriture engendrée par la cloture contextuelle des règles suivantes :

Coupure axiome :



Coupure multiplicative :