Théorie de la démonstration

Examen final (avec corrigé)

3 mai 2012

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

Barème. Les copies ont été notée de la manière suivante. Les exercices qui n'ont été faits/essayés par personne ont été exclus du barème (ils comptent 0). On reste donc avec les exercices suivants, avec leur valeur respectif :

1.	4 points ;
2a.	1 point ;
2b.	3 points ;
2c.	2 points ;
2d.	3 points ;
2e.	2 points ;
3a.	2 points ;
4a.	2 points ;
4b.	2 points (on ne compte que la toute première partie, c'est-à-dire, la fonction $X \mapsto X^{\perp}$).

Cela fait donc un total de 21 points. La note finale est calculée en sommant les points obtenus pour chaque exercice et en reportant le résultat sur 20. Par exemple, une copie contenant une execution parfaite de la totalité des exercices 1 et 2, et rien d'autre, aura la note 15/20.

Pour brévité, je donnerai les corrigés détaillés seulement pour les exercices mentionnés ci-dessus.

Exercice 1. (Une loi de De Morgan) Donner une preuve en **NK** (déduction naturelle classique) de l'une des deux *lois de De Morgan*

$$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$$

(où la formule $A \Leftrightarrow B$ est définie comme $(A \Rightarrow B) \wedge (B \Rightarrow A)$).

Corrigé. Cet exercice a été resolu parfaitement par tout le monde, ce n'est pas la peine que j'en donne le corrigé.

Exercice 2. (Logique linéaire multiplicative intuitionniste) Dans la suite, on dénote par **MLL** le fragment purement multiplicatif de la logique linéaire, ainsi que son calcul des séquents.

La *logique linéaire multiplicative intuitionniste* (**IMLL**) est définie par les formules

$$A, B ::= X \mid 1 \mid A \otimes B \mid A \multimap B,$$

et son calcul des séquents par les règles

$$\frac{}{A \vdash A} \qquad \frac{\Gamma \vdash A}{\Gamma, 1 \vdash A} \qquad \frac{}{\vdash 1}$$

$$\frac{\Gamma, A, B \vdash C}{\Gamma, A \otimes B \vdash C} \qquad \frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \otimes B}$$

$$\frac{\Gamma \vdash A \quad \Delta, B \vdash C}{\Gamma, \Delta, A \multimap B \vdash C} \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \multimap B}$$

(La règle de l'échange est implicite. Il y a aussi la règle de la coupure, mais elle ne sera pas considérée ici ; le théorème d'élimination des coupures est valable pour **IMLL** aussi).

On rappelle que, dans **MLL**, la formule $A \multimap B$ est définie par $A^\perp \parr B$.

Soit R une formule de **MLL**. On pose $\neg_R A = A \multimap R$ et on définit :

$$\begin{array}{rcl} [X]_R & = & X \\ [X^\perp]_R & = & \neg_R X \\ [1]_R & = & 1 \\ [A \otimes B]_R & = & \neg_R \neg_R [A]_R \otimes \neg_R \neg_R [B]_R \\ [\bot]_R & = & \neg_R 1 \\ [A \parr B]_R & = & \neg_R (\neg_R [A]_R \otimes \neg_R [B]_R) \end{array}$$

a. Montrer que si R est une formule de **IMLL** alors $[A]_R$ l'est aussi (ce n'est pas forcement le cas si R est une formule de **MLL**).

b. Montrer que A et $[A]_\perp$ sont équivalentes dans **MLL**.

c. Montrer qu'il existe une formule A de **MLL** et une formule R de **IMLL** telles que A et $[A]_R$ ne sont pas équivalentes dans **MLL**.

d. Montrer que si $\vdash \Gamma$ est prouvable dans **MLL** et R est une formule de **IMLL** alors $[\vdash \Gamma]_R = \neg_R [\Gamma]_R \vdash R$ est prouvable dans **IMLL**.

e. Montrer que si $[\vdash \Gamma]_X$ est prouvable dans **IMLL** (avec X n'apparaissant pas dans Γ) alors $\vdash \Gamma$ est prouvable dans **MLL**.

Corrigé.

a. On constate immédiatement à partir de la définition de **IMLL** que si F et R sont des formules de **IMLL** alors $\neg_R F$ et $\neg_R \neg_R F$ le sont aussi. Le résultat s'obtient donc par une induction triviale sur A (formule de **MLL**).

b. Par définition, A et B sont *équivalentes* quand on peut prouver (en **MLL**) les séquents $\vdash A^\perp, B$ et $\vdash B^\perp, A$. On démontre immédiatement en calcul des séquents, par des dérivations d'au plus trois/quatre règles et sans devoir appliquer d'induction, que :

(a) si A', B' sont équivalentes respectivement à A, B, alors $A' \otimes B'$ est équivalente à $A \otimes B$;

(b) pour toute A, les formules $\neg_\perp A$ et $\neg_\perp \neg_\perp A$ sont équivalents respectivement à $A^\perp$ et A.

Le résultat est une conséquence immédiate des deux faits ci-dessus, en considérant la définition inductive de $[\cdot]_\perp$ (modulo le fait que, par définition, $(A^\perp \otimes B^\perp)^\perp = A \parr B$).

c. Tout le monde a su trouver un exemple (comme $A = \bot$ et $R = 1$).

d. La preuve est par induction sur la dernière règle de la dérivation de $\vdash \Gamma$. Tout le monde a bien développé ce point, pas la peine de donner les détails.

e. Personne n'a su donner de preuve satisfaisante. La première chose qu'on peut remarquer, c'est que, par définition, $[\vdash \Gamma]_X$ est toujours de la forme

$$A_1 \multimap X, \ldots, A_n \multimap X \vdash X,$$

c'est-à-dire, il s'agit d'un séquent contenant un atome à droite et des implications à gauche. Cela veut dire qu'une preuve par induction sur la dernière règle de la dérivation de $[\vdash \Gamma]_X$ ne pourra pas marcher, car le seul cas qui s'appliquerait serait la flèche à gauche, auquel on ne pourrait pas appliquer l'hypothèse d'induction ensuite (car on tomberait sur un séquent qui n'est pas forcement de la forme ci-dessus). On procède alors comme suit. On commence par démontrer que, dans **MLL** :

(a) $(A[\bot/X])^\bot = A^\bot[\bot/X]$ (facile, par induction sur A) ;

(b) $\vdash \Gamma$ prouvable implique $\vdash \Gamma[\bot/X]$ prouvable (immédiat, par induction sur la dernière règle de la dérivation, en utilisant (a)) ;

(c) si X n'apparaît pas dans A, $[A]_\bot = ([A]_X)[\bot/X]$ (induction facile).

Soit maintenant $\Gamma = A_1, \ldots, A_n$. On a

$$[\vdash \Gamma]_X = [A_1]_X \multimap X, \ldots, [A_n]_X \multimap X \vdash X.$$

Si ce séquent est prouvable dans **IMLL** alors le séquent

$$\vdash [A_1]_X \otimes X^\bot, \ldots, [A_n]_X \otimes X^\bot, X$$

est prouvable dans **MLL**, car **IMLL** se plonge dans **MLL** de la façon évidente (le séquent $\Gamma \vdash A$ de **IMLL** correspondant au séquent $\vdash \Gamma^\bot, A$ de **MLL**, avec le connecteur $\multimap$ défini à travers le $\parr$). Grâce au points (b) et (c), on a que

$$\vdash [A_1]_\bot \otimes 1, \ldots, [A_n]_\bot \otimes 1, \bot$$

est dérivable dans **MLL**. Mais la dérivabilité de ce séquent est équivalente à la dérivabilité de

$$\vdash [A_1]_\bot, \ldots, [A_n]_\bot,$$

car 1 et $\bot$ sont les éléments neutres de $\otimes$ et $\parr$, respectivement. Or, on a démontré au point **b** de cet exercice que, pour toute A, $[A]_\bot$ est équivalente à A, donc le séquent ci-dessus est en effet équivalent à $\vdash \Gamma$, et la prouvabilité du premier implique la prouvabilité de ce dernier.

Exercice 3. (Élimination des coupures dans les réseaux) On rappelle qu'un *multiensemble* sur un ensemble E est une fonction $M : E \to \mathbb{N}$. On écrit $x \in M$ si $M(x) > 0$. La somme de deux multiensembles sur E est définie de manière évidente (point par point). On écrit $N \sqsubseteq M$ si pour tout $x \in E$, $N(x) \leq M(x)$. Si $N \sqsubseteq M$, on définit la différence $M - N$ de la même manière que la somme (point par point). Dans la suite, quand on écrit $M - N$ on suppose implicitement que $N \sqsubseteq M$.

Si E est muni d'un ordre partiel $\preceq$, et si M, N sont deux multiensembles sur E, on définit

$$M \preceq_m N \quad \text{si} \quad M = (N - X) + Y,$$

où X, Y sont deux multiensembles sur E tels que X *domine* Y, c'est-à-dire,

$$\forall y \in Y,\ \exists x \in X \text{ t.q. } y \preceq x.$$

On peut démontrer que $\preceq_m$ est un ordre partiel qui est bien fondé lorsque $\preceq$ l'est.

On se place dans **MELL**, le fragment multiplicatif-exponentiel de la logique linéaire propositionnelle, sans unités (1 et $\bot$). Dans le reste du sujet, on travaillera exclusivement avec les réseaux ; aucune référence au calcul des séquents n'est admise.

Par *réseau* on entendra un réseau quelconque, ne satisfaisant pas forcement le critère de correction. Un réseau correct (satisfaisant le critère de correction) sera appelé *réseau de preuve*. On remarque que la correction n'est pas nécessaire pour définir les étapes d'élimination des coupures.

Même si les résultats suivants peuvent être prouvés en toute généralité, pour simplifier un petit peu les preuves ici on ne considérera pas l'étape commutative (boîte/boîte) de l'élimination des coupures.

a. Soient π, π' deux réseaux de **MELL** tels que $\pi \to \pi'$, c'est-à-dire, π' est obtenu à partir de π par application d'une étape d'élimination des coupures. Montrer que si π est un réseau de preuve alors π' l'est également. Pour cela, on utilisera l'*invariant d'Euler-Poincaré*, qui affirme que tout graphe non-dirigé G vérifie l'équation

$$v - e = k - c,$$

où v, e, k et c sont respectivement le nombre de noeuds, arêtes, composantes connexes et cycles de G.

b. Soit c une coupure d'un réseau π.
- Le *dégré* de c, noté par $\deg c$, est la complexité logique de ses prémisses ;
- le *rang* de c, noté par ∇c, est égal à 0 si c est une coupure axiome ou multiplicative ; s'il s'agit d'une coupure exponentielle, on procède comme suit. Par définition, c a une prémisse p de la forme $?A$; cette premisse induit un arbre qui a comme racine p elle-même et comme feuilles les conclusions des liens axiomes ou déréliction qui introduisent $?A$. On définit alors ∇c comme la hauteur de cette arbre.

Soit π un réseau contenant les coupures $c_1, \ldots, c_n$. On défini sa *mesure* $\mu(\pi)$ comme le multiensemble $[(\deg c_1, \nabla c_1), \ldots, (\deg c_n, \nabla c_n)]$.

Soit π un réseau de preuve. Montrer que, si π n'est pas sans coupure, il existe une coupure de π tel que, si $\pi \to \pi'$ par réduction de cette coupure, alors $\mu(\pi') \prec_m \mu(\pi)$, où l'on considère l'ordre sur les multiensembles défini ci-dessus, à partir de l'ordre lexicographique $\preceq$ sur les paires d'entiers naturels.

c. Soit π un réseau de preuve sans occurrences du connecteur « ! » dans ses conclusions. Montrer que si π n'est pas sans coupures alors il existe une coupure non-commutative.

d. À partir des points **a**, **b** et **c** ci-dessus, déduire la suivante version restreinte du théorème d'élimination des coupures : tout réseaux de preuve sans « ! » dans ses conclusions admet une forme sans coupures de mêmes conclusions.

Corrigé.

a. L'exercice supposait la définition de réseau de preuve que j'avais donnée en cours, en absence de quantificateurs, c'est-à-dire, un réseau de preuve est un réseau dont tout graphe de correction est acyclique, où les graphes de correction sont obtenus en « écrasant » les boîtes en un seul nœud et en supprimant une prémisse au choix pour chaque « par » et « contraction ». Néanmoins, avec l'exception du cas affaiblissement, les arguments fonctionnent de manière identique si l'on considère aussi la condition de connexion.

On appellera G' le graphe de correction générique de π', dont il faudra (et suffira de) vérifier l'acyclicité. On dénotera par v', e' et k' le nombre de nœuds, arêtes et composantes connexes de G'. On remarque que G' induit un certain nombre de graphes de correction $G_1, \ldots, G_n$ de π, qui font « les mêmes choix » que G' sur les nœuds en commun. On observe que tous ces graphes de correction ont le même nombre de nœuds, arêtes et composantes connexes, que l'on dénotera par v, e et k.

On a 5 étapes d'élimination des coupures à analyser : axiome, multiplicatif, déréliction, contraction, affaiblissement. Dans tous les cas, on peut imaginer que la coupure se trouve à profondeur zéro de π ; si elle est à l'intérieur d'une boîte, le raisonnement est identique et s'applique à la correction de la boîte elle-même (on rappelle que le contenu de chaque boîte de π doit lui aussi satisfaire le critère de correction).

axiome : G' induit exactement un graphe de correction G_1 de π, qui a exactement les même chemins. G' est donc acyclique.

multiplicatif : G' induit deux graphes de correction G_1, G_2, selon le choix que l'on fait sur le « par » impliqué dans la coupure. Indépendemment de ce choix, on a $v = v_0 + 3$ et $e = e_0 + 5$ (une arête du « par » est supprimée par le switching), alors que $v' = v_0 + 2$ et $e' = e_0 + 4$, donc $v' - e' = v - e$. À ce moment là, on remarque que le nombre de composantes connexes de G_i et G' est le même, donc G' est acyclique puisque les G_i le sont.

déréliction : Dans ce cas aussi, G' induit exactement un graphe de correction G_1. Si l'on dénote par p le nombre de portes auxiliaires de la boîte impliquée dans la coupure, on a

$$\begin{aligned} v &= v_0 + 3 \\ e &= e_0 + p + 3 \\ k &= k_0 + 1 \end{aligned}$$

car la boîte est « écrasée » en un nœud et on a au moins une composante connexe. Dans G', on a la situation suivante :

$$\begin{aligned} v' &= v_0 + v_1 + 1 \\ e' &= e_0 + p + 1 + e_1 + 1 \\ k' &= k_0 + k_1, \end{aligned}$$

où v_1, e_1 et k_1 sont le nombre de nœuds, arêtes et composantes connexes du graphe de correction associé au contenu de la boîte qui

a été « ouverte » par l'exécution de l'étape (en effet, la composante connexe qui contient la coupure dans π se retrouve découpée en k_1 composantes connexes après l'ouverture de la boîte). Comme π est correct, on a $v - e - k = 0$ et $v_1 - e_1 - k_1 = 0$. En utilisant ces équations, on arrive facilement a déduire $v' - e' - k' = 0$ aussi, donc G' est acyclique.

contraction : On remarque que, comme dans le cas multiplicatif, G' induit deux graphes de correction G_1, G_2, dont le nombre de composantes connexes est le même que celui de G'. Si la boîte impliquée dans la coupure a p portes auxiliaires, on a $v = v_0+3$ et $e = e_0+p+3$, alors que $v' = v_0 + 4 + p$ et $e' = e_0 + 2p + 4$, donc $v' - e' = v - e$ et G' est acyclique car G_1 et G_2 le sont.

affaiblissement. C'est immédiat : G' induit un unique graphe de correction G_1, acyclique par hypothèse, qui a strictement plus de chemins que G' ; ce dernier est donc acyclique.

b. La seule propriété qu'il fallait retenir concernant l'ordre sur les multiensembles est la suivante : pour tout multiset M est pour tout $x, y_1, \ldots, y_n$ tels que $y_i \prec x$ pour tout $1 \leq i \leq n$, on a

$$M + [y_1, \ldots, y_n] \prec_m M + [x].$$

Autrement dit, on peut « retirer » un élément d'un multiensemble et le « remplacer » par n'importe combien d'éléments strictement plus petits pour obtenir un multiensemble strictement plus petit que celui de départ. Il suffit alors d'observer les étapes d'élimination des coupures pour constater que, si x est la mesure de la coupure éliminée et si $y_1, \ldots, y_n$ sont les mesures des coupures introduites par l'étape, on est toujours dans la situation mentionnée ci-dessus.

c. Il faut utiliser l'acyclicité ; je ne donne pas de détail ici.

d. Soit π un réseau de preuve sans « ! » dans les conclusions n'admettant pas de réduction finie. Grâce à **a**, tous les réduits de π sont aussi des réseaux de preuve, donc on peut toujours appliquer **c**, qui nous garantit l'existence d'une coupure non-commutative dans chacun de ces réseaux ; de plus, **b** nous garantit qu'au moins une de ces coupures fait décroitre strictement la mesure. Mais on aurait alors une chaine infinie strictement décroissante dans l'ordre $\preceq_m$, une contradiction.

Excercice 4. (Construction d'un modèle du λ-calcul pur) Soient X, Y deux espaces cohérents. On définit $X \sqsubseteq Y$ si :

i) $|X| \subseteq |Y|$;

ii) $\forall a, a' \in |X|$, $a \frown_X a'$ ssi $a \frown_Y a'$.

a. Montrer que l'ensemble [1] des espaces cohérents, ordonné par $\sqsubseteq$, est un ω-cpo, c'est-à-dire :
– il existe un plus petit élément ;

1. Techniquement, pour que ce ne soit pas une classe propre, il faut se restreindre à des espaces cohérents dont les trames sont toutes contenues dans un ensemble donné à l'avance. Ce détail n'a aucune importance dans ce qui suit.

– toute chaine croissante $(X_n)_{n<\omega}$ d'espaces cohérents a une plus petite borne supérieure, que l'on notera $\bigvee_{n<\omega} X_n$.

b. Montrer que les fonctions suivantes sont continues (au sens de Scott) :
– $X \mapsto X^\perp$;
– $X \mapsto !X$;
– $X \mapsto X^{\mathbb{N}}$, où $X^{\mathbb{N}}$ est le produit d'un nombre dénombrable de copies de X, c'est-à-dire :
  – $|X^{\mathbb{N}}| = \bigcup_{i<\omega} \{i\} \times |X|$;
  – $(i,a) \frown_{X^{\mathbb{N}}} (j,b)$ ssi $i \neq j$ ou $i = j$ et $a \frown_X b$.

On rappelle qu'un fonction F est continue si pour toute chaine croissante $(X_n)_{n<\omega}$, $F(\bigvee_{n<\omega} X_n) = \bigvee_{n<\omega} F(X_n)$.

c. Trouver des espaces cohérents qui vérifient les isomorphismes suivants :
– $A \cong A^\perp$;
– $B \cong !B$;
– $D = (!D^{\mathbb{N}})^\perp$.

d. Montrer que l'espace cohérent D du point précédent vérifie, de plus, l'isomorphisme

$$D \cong !D \multimap D.$$

Que peut-on conclure sur D ?

Corrigé.

a. Soit $(X_n)_{n<\omega}$ une chaine croissante. On pose

$$\begin{array}{rcl} |Y| & = & \bigcup_{n<\omega} |X_n|, \\ x \frown_Y x' & \text{ssi} & \exists n.\ x \frown_{X_n} x'. \end{array}$$

Il est immédiat de vérifier que $\bigvee_{n<\omega} X_n = (|Y|, \frown_Y)$. L'espace cohérent vide est évidemment le plus petit élement.

b. Soit $(X_n)_{n<\omega}$ une chaine croissante. On fixe les notations

$$Y = (\bigvee_{n<\omega} X_n)^\perp, \qquad Y' = \bigvee_{n<\omega} X_n^\perp.$$

Il suffit de démontrer que $Y = Y'$. Évidemment $|Y| = |Y'| = \bigcup_{n<\omega} |X_n|$, il reste donc à montrer que la cohérence est identique. Pour cela, on remarque que, à cause de la définition d'ordre, on a $\exists n.\ x \asymp_{X_n} x'$ ssi $\forall n.\ x \asymp_{X_{n'}} x'$. En effet, si $x = x'$, c'est trivial ; si $x \neq x'$ et il existe n_0 t.q. $x \asymp_{X_{n_0}} x'$, alors $x \asymp_{X_n} x'$ pour tout n, car soit x, x' ne sont pas les deux dans $|X_n|$, soit $|X_{n_0}| \subseteq |X_n|$ et l'incohérence est préservée. On a alors $x \frown_Y x'$ ssi $x \asymp_{\bigvee_{n<\omega} X_n} x'$ ssi $\forall n.\ x \asymp_{X_{n'}} x'$ ssi $\exists n.\ x \asymp_{X_n} x'$ ssi $x \frown_{Y'} x'$.
Je ne donne pas de détail pour les autres deux fonctions.

c. Il suffit de se rappeler du théorème de point fixe de Kleene : toute fonction continue sur un cpo a un point fixe, que l'on construit par des applications successives de la fonction elle-même, à partir de l'élément minimum. On a démontré au point **b** que $(\cdot)^\perp$, $!(\cdot)$ et $(!(\cdot)^{\mathbb{N}})^\perp$ sont continues, donc on peut trouver des reponses à la question par application successive de ces fonctions, à partir de l'espace cohérent vide.

Pour la première question, cela se fait immédiatement : l'espace cohérent vide est le dual de lui-même. Pour la fonction $X \mapsto !X$, on voit facilement que, à l'n-ème itération, on obtient un espace cohérent dont la trame a 2^n points tous cohérents entre eux. Il est donc clair que si l'on définit $N = (\mathbb{N}, \mathbb{N} \times \mathbb{N})$ (un espace à trame dénombrable dont tous les points sont cohérents entre eux), on a $!N \cong N$, comme on peut vérifier aisement. Je ne donne pas de détail pour le troisième point.

d. Ce point est assez difficile, je ne donne pas de détail. En tout cas, la conclusion est, évidemment, que D est un modèle du λ-calcul pur.