Théorie de la démonstration

Examen final

9 avril 2014

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

Exercice 1. (Loi de Peirce et implication contraposée) Soit $\mathbf{NJ}_{\text{Peirce}}$ la déduction naturelle intuitionniste à laquelle on rajoute la possibilité d'utiliser des axiomes de la forme

$$\dfrac{}{((A \Rightarrow B) \Rightarrow A) \Rightarrow A}$$

pour n'importe quelles formules A et B.

Montrer que la formule $(\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$ est prouvable en $\mathbf{NJ}_{\text{Peirce}}$.

Corrigé. Voici une preuve possible :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{(\neg B \Rightarrow B) \Rightarrow B}\,\text{Peirce} \qquad \dfrac{\dfrac{\dfrac{\dfrac{[\neg B \Rightarrow \neg A]^{\#} \quad [\neg B]^{*}}{\neg A}\,{\Rightarrow}\mathrm{E} \qquad [A]^{\dagger}}{\bot}\,{\Rightarrow}\mathrm{E}}{B}\,\bot\mathrm{E}}{\neg B \Rightarrow B}\,{\Rightarrow}\mathrm{I}*}{B}\,{\Rightarrow}\mathrm{E}}{A \Rightarrow B}\,{\Rightarrow}\mathrm{I}\dagger}{(\neg B \Rightarrow \neg A) \Rightarrow A \Rightarrow B}\,{\Rightarrow}\mathrm{I}\#$$

Exercice 2. (Typabilité dans le Système F) On considère le système F à la Curry, rappelé dans la suite. Le types sont engendrés par

$$A, B ::= X \mid A \to B \mid \forall X.A.$$

On définit un *contexte* comme une suite de la forme

$$x_1 : A_1, \ldots, x_n : A_n,$$

où les x_i sont des variables deux à deux distinctes et les A_i sont des types. Un *jugement* est une expression de la forme

$$\Gamma \vdash M : A$$

où M est un λ-terme pur (c'est-à-dire, sans annotations de type), A est un type et Γ est un contexte (contenant les variables libres de M). Les jugements peuvent être dérivés à partir des règles suivantes :

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

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

$$\frac{\Gamma \vdash M : A}{\Gamma \vdash M : \forall X.A} \; X \text{ n'est pas libre dans } \Gamma \qquad \frac{\Gamma \vdash M : \forall X.A}{\Gamma \vdash M : A[B/X]}$$

a. Démontrer le *lemme de substitution* suivant : pour tous λ-termes M et N, si les jugements

$$\Gamma, x : A \vdash M : B,$$
$$\Gamma \vdash N : A$$

sont dérivables, alors

$$\Gamma \vdash M[N/x] : B$$

est dérivable.

Corrigé. La preuve est par induction sur la dernière règle de la dérivation du jugement $\Gamma, x : A \vdash M : B$:

axiome : dans ce cas $M = y$, et $M[N/x] = N$ si $y = x$ ou $M[N/x] = y$ si $y \neq x$. Ce dernier cas est trivial et dans le premier cas on conclut grâce à l'hypothèse $\Gamma \vdash N : A$;

flèche intro : dans ce cas $A = A' \to A''$, $M = \lambda y.M'$ et $M[N/x] = \lambda y.M'[N/x]$. Nous avons $\Gamma, y : A' \vdash M'[N/x] : A''$ par hypothèse d'induction et on peut donc conclure ;

flèche elim : dans ce cas $M = M'M''$ et $M[N/x] = M'[N/x]M''[N/x]$. Nous avons $\Gamma \vdash M'[N/x] : A' \to A$ et $\Gamma \vdash M''[N/x] : A'$ par hypothèse d'induction, ce qui nous permet de conclure ;

pour tout intro et elim : ces deux cas sont une conséquence immédiate de l'hypothèse d'induction.

b. En déduire la propriété de *réduction du sujet* : pour tous λ-termes M, M' tels que $M \to_\beta M'$, si

$$\Gamma \vdash M : A$$

est dérivable, alors

$$\Gamma \vdash M' : A$$

est dérivable.

Corrigé. La plupart des copies ici ont supposé que $M = (\lambda x.P)N$, ce qui est faux en géneral : le redex réduit peut se trouver n'importe où à l'intérieur de M. Cela ne pose cependant aucun problème, la preuve se fait toujours par induction sur sur la dernière règle de la dérivation du jugement $\Gamma \vdash M : A$:

axiome : impossible (car $M = x$ serait en forme normale) ;

flèche intro : dans ce cas $A = A' \to A''$, $M = \lambda x.M_1$, $\Gamma, x : A' \vdash M_1 : A''$ est dérivable et nous avons forcement que $M' = \lambda x.M_1'$ avec $M_1 \to_\beta M_1'$. L'hypothèse d'induction nous donne $\Gamma, x : A' \vdash M_1' : A''$, d'où on conclut ;

flèche elim : dans ce cas $M = M_1 N$ et $\Gamma \vdash M_1 : B \to A$ et $\Gamma \vdash N : B$ sont dérivables. On a trois sous-cas :

– $M' = M'_1 N$ avec $M_1 \to_\beta M'_1$: on conclut facilement par hypothèse d'induction ;
– $M' = M_1 N'$ avec $N \to_\beta N'$: analogue au cas précédent ;
– $M_1 = \lambda x.M_2$ et $M' = M_2[N/x]$: dans ce cas, le type de M_1 nous assure que $\Gamma, x : B \vdash M_2 : A$ est dérivable, donc on peut conclure en applicant le lemme de substitution (point a) ;

pour tout intro et elim : ces deux cas sont une conséquence immédiate de l'hypothèse d'induction.

c. Soient $\Delta := \lambda x.xx$ et $M := (\lambda x.y)(\Delta\Delta)$. Est-ce que M est typable dans le système F ?

Corrigé. Non, car on sait que tout terme typable dans le système est fortement normalisable ; or, $M \to_\beta M$ en réduisant le rédex $\Delta\Delta$, ce qui montre qu'il existe une réduction infinie à partir de M.

d. L'*expansion du sujet* pour un système de types est la propriété suivante : pour tous λ-termes M, M' tels que $M \to_\beta M'$, si

$$\Gamma \vdash M' : A$$

est dérivable, alors

$$\Gamma \vdash M : A$$

est dérivable. Est-ce que le système F juit de cette propriété ?

Corrigé. Non, le terme M du point c nous fournit un contrexemple : nous avons $M \to_\beta y$; or, y est évidemment typable, alors que M ne l'est pas.

e. Soit $\bot := \forall X.X$. Dériver le jugement suivant :

$$\vdash \Delta : \bot \to \bot.$$

Corrigé. En voici une dérivation :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{x : \bot \vdash x : \bot}}{x : \bot \vdash x : \bot \to \bot} \quad \dfrac{}{x : \bot \vdash x : \bot}}{x : \bot \vdash xx : \bot}}{\vdash \Delta : \bot \to \bot}$$

f. Prouver que tout λ-terme en forme normale est typable. Plus précisement, démontrer qu'il existe un type B tel que, pour tout λ-terme M en forme normale dont les variables libres sont parmi $x_1, \dots, x_n$, il existe un type A engendré par

$$A ::= B \mid A \to B$$

tel que le jugement

$$x_1 : B, \dots, x_n : B \vdash M : A$$

est dérivable. (*Suggestion : généralisez la solution du point* e *et utilisez l'observation que, puisqu'il est normal, M est toujours de la forme*

$$\lambda y_1 \dots \lambda y_m.zN_1 \cdots N_k,$$

où $z \in \{y_1, \ldots, y_m, x_1, \ldots, x_n\}$ et $N_1, \ldots, N_k$ sont eux-mêmes normaux).

Corrigé. Le point précédent nous suggère de prendre $B = \bot$. On procède par induction sur M, qui est de la forme donnée ci-dessus. Soient $\Gamma := x_1 : \bot, \ldots, x_n : \bot$ et $\Delta := y_1 : \bot, \ldots, y_m : \bot$. L'hypothèse d'induction nous donne, pour chaque $1 \leq i \leq k$, un type A_i de la forme voulue tel que $\Gamma, \Delta \vdash N_i : A_i$. Nous pouvons donc écrire

$$\dfrac{\dfrac{\begin{array}{c}\dfrac{\dfrac{\dfrac{}{\Gamma, \Delta \vdash z : \bot}}{\Gamma, \Delta \vdash z : A_1 \to \cdots \to A_k \to \bot} \quad \Gamma, \Delta \vdash N_1 : A_1}{\Gamma, \Delta \vdash zN_1 : A_2 \to \cdots \to A_k \to \bot} \\ \vdots \end{array} \qquad \Gamma, \Delta \vdash N_k : A_k}{\Gamma, \Delta \vdash zN_1 \cdots N_k : \bot}}{\Gamma \vdash M : \bot \to \cdots \to \bot \to \bot}$$

et on conclut en observant que le type $\bot \to \cdots \to \bot \to \bot$ est bien de la forme désirée.

Exercice 3. (Vers la focalisation) On considère la logique linéaire multiplicative exponentielle, propositionnelle et sans unités (**MELL**), dont les formules sont engendrées par

$$A, B ::= X \mid X^\perp \mid A \otimes B \mid A \parr B \mid\, !A \mid ?A,$$

où X varie sur un ensemble d'atomes propositionnels. On dit qu'une formule est :

- *atomique* si elle est de la forme X ou $X^\perp$;
- *positive* si elle est de la forme $A \otimes B$ ou $!A$;
- *négative* si elle est de la forme $A \parr B$ ou $?A$.

Nous allons travailler avec des séquents de la forme

$$\vdash \Theta; \Gamma$$

où Θ, Γ sont comme d'habitude des multiensembles de formules. Nous dénoterons par Π, Π' des multiensembles ne contenant aucune formule négative. Sur ces séquents, on définit le calcul suivant, que l'on appelle **MELL′** :

$$\dfrac{}{\vdash \Theta; X^\perp, X} \qquad \dfrac{\vdash \Theta; \Pi, A \quad \vdash \Theta; \Pi', B}{\vdash \Theta; \Pi, \Pi', A \otimes B} \qquad \dfrac{\vdash \Theta; \Gamma, A, B}{\vdash \Theta; \Gamma, A \parr B}$$

$$\dfrac{\vdash \Theta; A}{\vdash \Theta; !A} \qquad \dfrac{\vdash \Theta, A; \Gamma}{\vdash \Theta; \Gamma, ?A} \qquad \dfrac{\vdash \Theta, A; \Pi, A}{\vdash \Theta, A; \Pi}$$

a. Démontrer que $\vdash \Theta; \Gamma$ dans **MELL′** implique $\vdash ?\Theta, \Gamma$ dans **MELL**.

   Corrigé. Par induction sur la dernière règle de la dérivation de $\vdash \Theta; \Gamma$. Tout le monde a plus ou moins bien développé ce point, ce n'est pas la peine que j'en donne le corrigé.

b. Démontrer que si $\vdash \Gamma$ est dérivable dans **MELL**, alors il est dérivable dans **MELL** en n'utilisant que des axiomes atomiques (c'est-à-dire, de la forme $\vdash X^\perp, X$).

Corrigé. Tout le monde a su développer ce point, même si seulement dans 2 copies on s'est rendu compte qu'il n'y en fait que 3 cas, et non pas 5, car l'induction ne se fait pas sur la formule mais sur la complexité logique de la paire $A, A^\perp$ introduite par l'axiome (A et $A^\perp$ ont la même taille car elles sont duales). On a donc :

- A et $A^\perp$ atomiques : rien à faire ;
- A et $A^\perp$ multiplicatives : par symétrie, on peut supposer sans perte de généralité que $A = A_1 \otimes A_2$ et produire la dérivation

$$\dfrac{\dfrac{\dfrac{}{\vdash A_1^\perp, A_1} \quad \dfrac{}{\vdash A_2^\perp, A_2}}{\vdash A_1^\perp, A_2^\perp, A_1 \otimes A_2}}{\vdash A_1^\perp \parr A_2^\perp, A_1 \otimes A_2}$$

- A et $A^\perp$ exponentielles : par symétrie, on peut supposer sans perte de généralité que $A = {!A'}$ et produire la dérivation

$$\dfrac{\dfrac{\dfrac{}{\vdash {A'}^\perp, A'}}{\vdash ?{A'}^\perp, A'}}{\vdash ?{A'}^\perp, !A'}$$

c. Soit δ une dérivation de **MELL** et soit δ' obtenue par élimination des coupures à partir de δ. Si δ n'utilise que des axiomes atomiques, est-ce que δ' en utilise ?

Corrigé. Tout le monde a observé corectement que l'élimination des coupure propositionnelle ne modifie pas la complexité des axiomes, donc δ' aussi n'a que d'axiomes atomiques.

J'observe ici que la situation changerait si on était aux second ordre : dans ce cas, l'élimination d'une coupure entre $\forall X.A$ et $\exists X.A^\perp$, où le témoin de l'existentiel est B non-atomique, substituirait partout dans la preuve la formule B à l'atome X, ce qui pourrait transformer un axiome atomique introduisant $X^\perp, X$ en un axiome non-atomique $B^\perp, B$.

d. Soit Σ obtenu par décomposition de tous les connecteurs $\parr$ de Γ, c'est-à-dire, on transforme tout $A \parr B$ dans Γ en A, B jusqu'à ce qu'il ne reste que des formules dont le connecteur principal n'est pas un $\parr$ (par exemple, si $\Gamma = X \parr ?(A \parr B), (Y \parr Z) \parr !C, D \otimes E$, nous avons $\Sigma = X, ?(A \parr B), Y, Z, !C, D \otimes E$). Montrer que si $\vdash \Gamma, \Delta$ est dérivable dans **MELL**, alors $\vdash \Sigma, \Delta$ l'est aussi et que, de plus, le nombre de règles de la deuxième dérivation n'est pas supérieur à celui de la première (en fait, il est strictement inférieur lorsqu'il y a au moins une formule $\parr$ dans Γ).

Corrigé. À partir de ce moment, on peut se placer dans **MELL** sans coupures et avec axiomes atomiques, le points b e c nous assurant que l'on ne perd rien en prouvabilité.

Pour le point d, il suffit de montrer que la règle

$$\dfrac{\vdash \Phi, A \parr B}{\vdash \Phi, A, B}$$

est admissible dans **MELL** et qu'elle n'augmente pas la taille des preuves ; le résultat suit par application successive de cette règle au séquent $\vdash \Gamma, \Delta$.

On fait cela par induction sur la dernière règle de la preuve de $\vdash \Phi, A \parr B$. Cela ne peut pas être un axiome, car il ne serait pas atomique, ni une promotion, car il n'y aurait pas de $\parr$ dans la conclusion. Le cas d'une règle $\parr$ nous donne immédiatement le résultat attendu : $\vdash \Phi, A, B$ est dérivable, avec une règle de moins. Les cas d'une règle $\otimes$, d'une déréliction, d'une contraction ou d'un affaiblissement sont une conséquence immédiate de l'hypothèse d'induction, car $A \parr B$ est dans le contexte de ces règles.

e. Montrer que les règles suivantes sont admissibles dans **MELL**$'$:

$$\frac{\vdash \Theta; \Gamma}{\vdash \Theta, A; \Gamma} \qquad \frac{\vdash \Theta, A, A; \Gamma}{\vdash \Theta, A; \Gamma} \qquad \frac{\vdash \Theta; \Gamma, ?A}{\vdash \Theta, A; \Gamma}$$

Corrigé. L'admissibilité de ces trois règles se montre aussi par une induction ne posant aucune difficulté, comme dans le point d.

f. En utilisant les points précédents (sauf a), démontrer que si $\vdash \Gamma$ est dérivable dans **MELL**, alors $\vdash ; \Gamma$ est dérivable dans **MELL**$'$.

Corrigé. Par induction sur la dernière règle de la dérivation de $\vdash \Gamma$ (que l'on peut supposer sans coupures et avec axiomes atomiques) :

axiome : immédiat ;

tenseur : si on applique bêtement l'hypthèse d'induction, on se retrouve avec une preuve de $\vdash ; \Gamma, A$ et une preuve de $\vdash ; \Delta, B$ et on est coincé. C'est pour cela qu'on a démontré le point d : à partir de la preuve de $\vdash \Gamma, A$ dans **MELL**, que l'on appelle δ, on sait qu'on peut obtenir une preuve de $\vdash ?\Theta, \Pi, A$, où $?\Theta, \Pi$ est la décomposition de tous les $\parr$ de Γ, avec Π ne contenant pas de formules négatives ; de plus, cette nouvelle dérivation n'est pas de taille supérieure à δ, donc on peut appliquer l'hypothèse d'induction et obtenir une dérivation de $\vdash ; ?\Theta, \Pi, A$ dans **MELL**$'$. De façon similaire, on obtient $\vdash ; ?\Theta', \Pi', B$ à partir de la deuxième premisse $\vdash \Delta, B$ ($?\Theta', \Pi'$ étant la décomposition de Δ). En appliquant les règles admissibles du point e, on a

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\vdash ; ?\Theta, \Pi, A}{\vdash \Theta; \Pi, A}}{\vdash \Theta, \Theta'; \Pi, A} \quad \cfrac{\cfrac{\vdash ; ?\Theta', \Pi', B}{\vdash \Theta'; \Pi', B}}{\vdash \Theta, \Theta'; \Pi', B}}{\vdash \Theta, \Theta'; \Pi, \Pi', A \otimes B}}{\vdash ; ?\Theta, \Pi, ?\Theta', \Pi', A \otimes B}}{\vdash ; \Gamma, \Delta, A \otimes B}\ \parr$$

par : immédiat ;

promotion : on utilise la troisième règle du point e :

$$\cfrac{\cfrac{\cfrac{\vdash ; ?\Gamma, A}{\vdash \Gamma; A}}{\vdash \Gamma; !A}}{\vdash ; ?\Gamma, !A}$$

déréliction : encore une fois, il faut faire recours au point d. À partir de $\vdash \Gamma, A$ dans **MELL**, on obtient une preuve (pas plus grande) de

$\vdash ?\Theta, \Pi, A$, où $?\Theta, \Pi$ est la décomposition de Γ. On applique l'hypothèse d'induction, qui nous fournit $\vdash ; ?\Theta, \Pi, A$ dans $\mathbf{MELL}'$. En utilisant le point **e**, on a donc

$$\begin{array}{c} \vdash ; ?\Theta, \Pi, A \\ \hline\hline \vdash \Theta ; \Pi, A \\ \hline \vdash \Theta, A ; \Pi, A \\ \hline \vdash \Theta, A ; \Pi \\ \hline\hline \vdash ; ?\Theta, \Pi, ?A \\ \hline\hline \vdash ; \Gamma, ?A \end{array} \;\; \parr$$

contraction : on utilise la contraction admissible, ansi que la troisième règle, du point **d** :

$$\begin{array}{c} \vdash ; \Gamma, ?A, ?A \\ \hline\hline \vdash A, A ; \Gamma \\ \hline \vdash A ; \Gamma \\ \hline \vdash ; \Gamma, ?A \end{array}$$

affaiblissement : on utilise l'affaiblissement admissible du point **d** :

$$\begin{array}{c} \vdash ; \Gamma \\ \hline \vdash A ; \Gamma \\ \hline \vdash ; \Gamma, ?A \end{array}$$