Correction du Partiel LOFO – Logique Formelle

EPITA – **Document, ordinateur et calculatrice ne sont pas autorisés**

Juin 2008 (1h30)

Le sujet et sa correction ont été écrits par Akim Demaille.

Une copie synthétique, bien orthographiée, avec un affichage clair des résultats, sera toujours mieux notée qu'une autre demandant une quelconque forme d'effort de la part du correcteur.

1 λ-calcul

Un λ-terme est une mot du langage suivant :

$$M \quad ::= \quad x \quad | \quad (\lambda x \cdot M) \quad | \quad (MM)$$

On rappelle les conventions suivantes :

— On omet les parenthèses extérieures $MN = (MN)$

— L'application associe à gauche $MNL = (MN)L$

— On peut grouper les abstractions imbriquées $\lambda xy \cdot M = \lambda x \cdot \lambda y \cdot M$

— L'abstraction capture le plus possible à droite $\lambda x \cdot MN = \lambda x \cdot (MN)$

Soit les deux combinateurs suivants :

$$\begin{aligned} \mathsf{Y} &= \lambda f \cdot (\lambda x \cdot f(xx))(\lambda x \cdot f(xx)) && \text{(Combinateur de Curry)} \\ \Theta &= (\lambda xy \cdot y(xxy))(\lambda xy \cdot y(xxy)) && \text{(Combinateur de Turing)} \end{aligned}$$

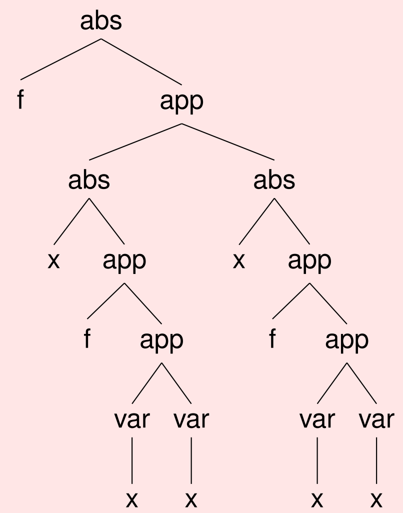
1. Écrire Y et Θ en les parenthésant complètement.

Correction:

$$\begin{aligned} \mathsf{Y} &= \lambda f \cdot ((\lambda x \cdot f(xx))(\lambda x \cdot f(xx))) \\ \Theta &= (\lambda xy \cdot y((xx)y))(\lambda xy \cdot y((xx)y)) \end{aligned}$$

2. Représenter l'arbre de syntaxe abstraite de Y en utilisant les constructeurs var, abs et app, et les noms des variables pour feuilles.

Correction:



3. Démontrer que ces combinateurs calculent les points fixes de fonction, c'est-à-dire que pour toute fonction g,
$$g\ (\mathsf{Y}\ g) = \mathsf{Y}\ g \qquad g\ (\Theta\ g) = \Theta\ g$$

Correction:

$$\begin{array}{rcl} \mathsf{Y}\ g & = & (\lambda f \cdot (\lambda x \cdot f(xx))(\lambda x \cdot f(xx)))\ g \\ & \to_\beta & (\lambda x \cdot g(xx))(\lambda x \cdot g(xx)) \\ & \to_\beta & g((\lambda x \cdot g(xx))(\lambda x \cdot g(xx))) \\ & \leftarrow_\beta & g(\lambda f \cdot ((\lambda x \cdot f(xx))(\lambda x \cdot f(xx)))g) \\ & = & g(\mathsf{Y}\ g) \end{array}$$

Posons $\theta = \lambda xy \cdot y((xx)y)$, i.e., $\Theta = \theta\theta$. Alors

$$\begin{array}{rcl} \Theta\ g & = & (\theta\theta)g \\ & = & (\lambda xy \cdot y((xx)y)\ \theta)\ g \\ & \to_\beta & \lambda y \cdot y((\theta\theta)y)\ g \\ & \to_\beta & g((\theta\theta)g) \\ & = & g(\Theta\ g) \end{array}$$

4. Supposons l'existence :
   — d'un codage des entiers en λ-calcul ($\underline{0}$, $\underline{1}$ etc.)
   — de la fonction pred (pred $\underline{n} = \underline{n-1}$ pour tout $n \geq 1$)
   — de la fonction mult (mult $\underline{n}\ \underline{m} = \underline{n \times m}$)
   — de la fonction ifzero (ifzero $\underline{n}\ M\ N = M$ si $n = 0, N$ sinon)
   — de la fonction fact qui prend un entier $\underline{n}$ et retourne $\underline{!n}$.
   En utilisant ces fonctions, écrire la définition récursive de fact.

Correction:
$$\mathsf{fact} = \lambda n \cdot \mathsf{ifzero}\, n(\underline{1})(\mathsf{mult}\, n(\mathsf{fact}(\mathsf{pred}\, n)))$$

5. Si f est une fonction récursive dont la valeur est M (i.e., le symbole f est lié à la valeur M, qui utilise le symbole f), on introduit $\overline{f} = \lambda f \cdot M$.

   Montrer que $\mathsf{Y}\ \overline{\mathsf{fact}}\ \underline{n}$ calcule $!n$.

Correction: On voulait dire définir ici

$$\overline{f} = \lambda\,\text{fact}\cdot\text{fact}$$

en quelque sorte, i.e. :

$$\begin{aligned}\overline{f} &= \lambda\,\text{fact}\cdot\lambda n\cdot\text{ifzero}\ n\ (\underline{1})\ (\text{mult}\ n\ (\text{fact}\ (\text{pred}\ n)))\\ &= \lambda f\cdot\lambda n\cdot\text{ifzero}\ n\ (\underline{1})\ (\text{mult}\ n\ (f\ (\text{pred}\ n)))\end{aligned}$$

2 λ-calcul Simplement Typé

Dérivations de type
Les dérivation de type sont construites à l'aide des nœuds suivants.

$$\dfrac{M:\sigma\to\tau \quad N:\sigma}{MN:\tau} \qquad \dfrac{\begin{matrix}[x:\sigma]\\ \vdots\\ M:\tau\end{matrix}}{\lambda x\cdot M:\sigma\to\tau}$$

1. Donner une déduction de type pour $\lambda xyz\cdot y$.

Correction: Deux façons de trouver la réponse : en devinant le résultat (ce qui est facile pour un informaticien) puis en le prouvant, ou bien partir de la dérivation « syntaxique » du terme (i.e. la partie à gauche des « : ») puis redescendre en attribuant des types et en résolvant les contraintes.

$$\dfrac{\dfrac{\dfrac{[y:\sigma]^1}{\lambda z\cdot y:\tau\to\sigma}}{\lambda y\cdot\lambda z\cdot y:\sigma\to\tau\to\sigma}\,1}{\lambda x\cdot\lambda y\cdot\lambda z\cdot y:\nu\to\sigma\to\tau\to\sigma}$$

Beaucoup d'étudiants sont perturbés par les abstractions faites sur des termes qui n'apparaissent pas au dessus, et inventent des dérivations comme suit :

$$\dfrac{[z:\tau]^1 y:\sigma}{\lambda z\cdot y:\tau\to\sigma}\,1$$

Je veux bien croire que LOFO ne soit pas un cours simple, mais s'il y a bien une chose facile, c'est de savoir si l'on est hors-sujet ou pas : les règles sont données, et il faut s'y tenir. Si vous ajoutez des règles **vous avez faux !**

2. Donner une déduction de type pour $\lambda xy\cdot xyy$.

Correction: Mêmes stratégies possibles que dans l'exercice précédent.

$$\dfrac{\dfrac{\dfrac{\dfrac{[x:\sigma\to\sigma\to\tau]^2[y:\sigma]^1}{xy:\sigma\to\tau} \qquad [y:\sigma]^1}{xyy:\tau}}{\lambda y\cdot xyy:\sigma\to\tau}\,1}{\lambda x\cdot\lambda y\cdot xyy:(\sigma\to\sigma\to\tau)\to\sigma\to\tau}\,2$$

Trop d'étudiants ont faux dès le début parce qu'ils n'ont pas su parenthéser correctement : $\lambda xy\cdot xyy = \lambda xy\cdot(xy)y \neq \lambda xy\cdot x(yy)$. Je donne 1/4 quand même quand la preuve est correcte.

3. Montrer que $\lambda xy\cdot yxy$ n'est pas typable.

4. Que pensez-vous de la typabilité de Y ?

Correction: On rappelle qu'en λ-calcul simplement typé, tout terme est fortement normalisable, et il est bien clair que des termes comme Y et Θ qui font des récursions, ne sont pas fortement normalisables. Il suffit par exemple de considérer la fonction succ, qui est typable, et d'en chercher le point fixe.

3 Calcul des Séquents Classique

Calcul des Séquents Classiques

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash \tau(\Delta)}\vdash X \quad \frac{\Gamma \vdash \Delta}{\sigma(\Gamma) \vdash \Delta}X\vdash \quad \frac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}\vdash W \quad \frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}W\vdash \quad \frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}\vdash C \quad \frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}C\vdash$$

$$\frac{}{F \vdash F}\mathrm{Id} \quad \frac{\Gamma \vdash A, \Delta \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\mathrm{Cut}$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\vdash\neg \quad \frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}\neg\vdash$$

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\vdash\wedge \quad \frac{\Gamma, A \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}l\wedge\vdash \quad \frac{\Gamma, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}r\wedge\vdash$$

$$\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A \vee B, \Delta}\vdash l\vee \quad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A \vee B, \Delta}\vdash r\vee \quad \frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\vee\vdash$$

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

Correction: Je m'attends bien entendu toujours à avoir des tentatives d'arnaques, mais certains sont des créatifs : des séquents sans symbole $\vdash$, voire plusieurs !
Certains ont utilisé d'autres règles (e.g., additives vs. multiplicatives) et en général je tolère.
Malheureusement plusieurs d'entre vous font des erreurs sincères et faciles à détecter. **Lisez** vos séquents, tout spécialement quand ils sont courts et faciles à comprendre. Si dans vos preuves apparaissent des choses comme $A \vee B \vdash A$ ou $A \vdash A \wedge B$, c'est *évidemment* faux !

1. Prouver l'équivalence entre $A \wedge (B \vee C)$ et $(A \wedge B) \vee (A \wedge C)$.

Correction: C'est triste à dire, mais beaucoup ne savent pas que pour prouver une équivalence, il faut prouver deux implications...
Prouvons $A \wedge (B \vee C) \vdash (A \wedge B) \vee (A \wedge C)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A}{A, B \vdash A} \quad \dfrac{B \vdash B}{A, B \vdash B}}{A, B \vdash A \wedge B}}{A, B \vdash (A \wedge B) \vee (A \wedge C)} \quad \dfrac{\dfrac{\dfrac{A \vdash A}{A, C \vdash A} \quad \dfrac{C \vdash C}{A, C \vdash C}}{A, C \vdash A \wedge C}}{A, C \vdash (A \wedge B) \vee (A \wedge C)}}{A, B \vee C \vdash (A \wedge B) \vee (A \wedge C)}}{A \wedge (B \vee C) \vdash (A \wedge B) \vee (A \wedge C)}$$

où je me suis permis dans la règle à double trait d'enchaîner deux introductions de $\wedge$ à gauche (qui donne deux fois $A \wedge (B \vee C)$) puis une contraction.

2. Prouver l'équivalence entre $A \vee (B \wedge C)$ et $(A \vee B) \wedge (A \vee C)$.
3. Vos preuves des questions 1 et 2 sont-elles intuitionnistes ?

Best-of: « Ces preuves sont intuitionnistes car elles n'utilisent pas la négation. »

4. Prouver $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$ (Loi de Peirce).

Correction:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{A \vdash A}}{A \vdash A, B}\,\vdash W}{\vdash A \Rightarrow B, A}\,\vdash\Rightarrow \qquad \overline{A \vdash A}}{(A \Rightarrow B) \Rightarrow A \vdash A, A}\,\Rightarrow\vdash}{(A \Rightarrow B) \Rightarrow A \vdash A}\,\vdash C}{\vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A}\,\vdash\Rightarrow$$

5. Votre preuve est-elle intuitionniste ?

Correction: Non, certains des séquents ont deux formules à droite (e.g., $A \vdash A, B$). Et effectivement, la loi de Peirce n'est pas (prouvable en logique) intuitionniste.

4 Déduction Naturelle Intuitionniste

$$\dfrac{\begin{matrix}[A]\\ \vdots \\ B\end{matrix}}{A \Rightarrow B}\,\Rightarrow\mathcal{I} \qquad \dfrac{A \quad A \Rightarrow B}{B}\,\Rightarrow\mathcal{E} \qquad \dfrac{\bot}{A}\,\bot\mathcal{E} \qquad \neg A := A \Rightarrow \bot$$

$$\dfrac{A \quad B}{A \wedge B}\,\wedge\mathcal{I} \qquad \dfrac{A \wedge B}{A}\,\wedge l\mathcal{E} \qquad \dfrac{A \wedge B}{B}\,\wedge r\mathcal{E}$$

$$\dfrac{A}{A \vee B}\,\vee l\mathcal{I} \qquad \dfrac{B}{A \vee B}\,\vee r\mathcal{I} \qquad \dfrac{A \vee B \qquad \begin{matrix}[A]\\ \vdots \\ C\end{matrix} \qquad \begin{matrix}[B]\\ \vdots \\ C\end{matrix}}{C}\,\vee\mathcal{E}$$

1. Prouver l'équivalence entre $A \wedge (B \vee C)$ et $(A \wedge B) \vee (A \wedge C)$.

Correction: Prouvons que $A \wedge (B \vee C) \vdash (A \wedge B) \vee (A \wedge C)$.

$$\dfrac{\dfrac{A \wedge (B \vee C)}{B \vee C} \qquad \dfrac{\dfrac{\dfrac{A \wedge (B \vee C)}{A} \quad [B]^1}{A \wedge B}}{(A \wedge B) \vee (A \wedge C)} \qquad \dfrac{\dfrac{\dfrac{A \wedge (B \vee C)}{A} \quad [C]^1}{A \wedge C}}{(A \wedge B) \vee (A \wedge C)}}{(A \wedge B) \vee (A \wedge C)}\,1$$

Montrons à présent la réciproque : $(A \wedge B) \vee (A \wedge C) \vdash A \wedge (B \vee C)$.

$$\dfrac{\dfrac{(A \wedge B) \vee (A \wedge C) \qquad \dfrac{[A \wedge B]^1}{A} \qquad \dfrac{[A \wedge C]^1}{A}}{A}\,1 \qquad \dfrac{(A \wedge B) \vee (A \wedge C) \qquad \dfrac{\dfrac{[A \wedge B]^2}{B}}{B \vee C} \qquad \dfrac{\dfrac{[A \wedge C]^2}{C}}{B \vee C}}{B \vee C}\,2}{A \wedge (B \vee C)}$$

2. Prouver $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$ (Loi de Peirce).

Correction: Cette formule n'est pas prouvable en logique intuitionniste.
Certains y sont parvenus *honnêtement* ! Comment faire ? Le prouver avec une tripotée d'hypothèses A non déchargées… En d'autres termes ils ont prouvé quelque chose comme $A \vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A$

Best-of:

$$\dfrac{\begin{array}{c}[A]^1\\ \vdots \\ B\end{array}}{A \Rightarrow B}\,1$$

Certains déchargent des conclusions…
Dans une des preuves, on trouve le morceau suivant :

$$\dfrac{\dfrac{[A]^1 \qquad A \Rightarrow B}{B}}{A \Rightarrow B}\,1$$

5 À propos de ce cours

Bien entendu je m'engage à ne pas tenir compte de ces renseignements pour vous noter. Ils ne sont pas anonymes, car je suis curieux de confronter vos réponses à votre note. En échange, quelques points seront attribués pour avoir répondu. Merci d'avance.

Répondre sur les formulaires de QCM. Vous pouvez cocher plusieurs réponses par question.

1. Assiduité
   - **a** Jamais venu
   - **b** Presque jamais venu
   - **c** Souvent venu
   - **d** Toujours présent
2. Travail personnel
   - **a** Rien
   - **b** Bachotage récent
   - **c** Relu les notes entre chaque cours
   - **d** Fait les anales
   - **e** Lu d'autres sources
3. Ce cours
   - **a** Est incompréhensible et j'ai rapidement abandonné
   - **b** Est difficile à suivre mais j'essaie
   - **c** Est facile à suivre une fois qu'on a compris le truc
   - **d** Est trop élémentaire

   Best-of: « Réponse c, et en l'occurrence ce n'est pas encore le cas en ce qui me concerne. »
4. Ce cours
   - **a** Ne m'a donné aucune satisfaction
   - **b** N'a aucun intérêt dans ma formation
   - **c** Est une agréable curiosité
   - **d** Je le recommande
5. L'enseignant
   - **a** N'est pas pédagogue
   - **b** Parle à des étudiants qui sont au dessus de mon niveau
   - **c** Me parle
   - **d** Se répète vraiment trop
   - **e** Se contente de trop simple et devrait pousser le niveau vers le haut