Correction du Partiel LOFO – Logique Formelle

EPITA – **Aucun document/ordinateur/calculatrice autorisé**

Décembre 2007 (1h30)

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

Désolé de ne pas avoir trouvé plus de temps pour vous rédiger une épreuve originale, ceux qui ont travaillé leurs anales ont certainement des facilités...

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.

Correction: Cet examen a été relativement bien réussi. J'ai noté généreusement, mais je ne suis pas aveugle : beaucoup ont appris bêtement les annales, y compris les erreurs qu'elles contenaient. Certains ont appris avec tant d'incompréhension que lorsque par un copier-coller j'avais laissé un "n-times" ou lieu d'un "n-fois", eh bien je l'ai retrouvé. En tout honnêteté je ne crois pas que ceux qui en sont là ont appris par cœur, je crois plutôt qu'ils ont triché.
D'autres éléments m'invite à penser que les brouillons ont circulé. Mais ce n'est pas à ce moment de votre scolarité que je vais jouer au flic.

1 λ-calculus

Dans ce sujet on s'intéresse aux « entiers de Church », une façon de coder les nombres naturels directement en λ-calculus, sans avoir à l'étendre avec de nouvelles constantes (comme `0` et `succ`).

L'idée est simple : les entiers de Church sont des fonctions de répétition. Le nombre de Church $\underline{0}$ applique 0 fois son argument fonction à un argument valeur, $\underline{42}$ le fait 42 fois. On pose :

$$\underline{n} = \lambda f \cdot \lambda x \cdot \underbrace{(f \cdots (f}_{n \text{ fois}}\, x \underbrace{) \cdots)}_{n \text{ fois}}$$

Correction: Mon sujet commençait bien mal, il était écrit :

$$\underline{n} = \lambda f \cdot \lambda x \cdot \underbrace{(f) \cdots (f)}_{n \text{ fois}}\, x$$

Ceci ne respecte pas l'associativité gauche de l'application de fonction: $f f x$ (ou $(f)(f)x$, les parenthèses ne changent bien sûr rien) se lit $(f f)x$. Dans ce cas, notre fonction f qui par exemple pourrait avoir un type $\alpha \to \alpha$ sera alimentée par f qui n'a pas le type α.

1. Écrire $\underline{2}$ et $\underline{3}$.

Correction:

$$\begin{aligned}\underline{2} &= \lambda f \cdot \lambda x \cdot f(fx)\\ \underline{3} &= \lambda f \cdot \lambda x \cdot f(f(fx))\end{aligned}$$

Vue l'erreur de l'énoncé, j'ai été *très* tolérant sur cette question, mais quand même pas au point d'accepter des choses comme $\underline{2} = f(fx)$.

2. Écrire une fonction succ qui prenne $\underline{n}$ et calcule $\underline{n+1}$.

Correction:

$$\text{succ} := \lambda n \cdot \lambda f \cdot \lambda x \cdot f(nfx)$$

Une réponse comme $\lambda n \cdot \lambda f \cdot fn$ ne convient pas: on a perdu f pour la suite. Ça se "sent" bien en regardant les types: f n'est pas appliquée sur une valeur comme x, mais sur un entier de Church.

3. Écrire une fonction plus qui prennent deux entiers $\underline{n}$ et $\underline{m}$ et calcule $\underline{n+m}$. Attention aux associativités.

Correction:

$$\text{plus} := \lambda n \cdot \lambda m \cdot \lambda f \cdot \lambda x \cdot mf(nfx)$$

Nombreux sont ceux qui ont recopié la correction (incorrecte) de 2005. Dommage. D'autres ont remarqué que faire une somme, c'est faire appel plusieurs fois au successeur, ce que les entiers de Church savent très bien faire:

$$\text{plus} := \lambda n \cdot \lambda m \cdot n \text{ succ } m$$

mais on n'a pas besoin de m ici.

$$\text{plus} := \lambda n \cdot n \text{ succ}$$

2 λ-calculus Simplement Typé

Type derivations are trees built from the following nodes.

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

1. Quel est le type de $\underline{1}$? Le prouver en fournissant l'arbre de preuve.

Correction: Bien sûr parler *du* type est abusif : on pensait au type principal. J'ai compté 1/4 pour ceux qui n'avait pas le type principal.

2. Quel est le type de $\underline{2}$? Le prouver en fournissant l'arbre de preuve.

Correction: Je retire 2/4 quand on ne mentionne pas les décharges.

3. Quel est le type de $\underline{n}$ pour $n > 2$? Le prouver.

Correction:

$$
\dfrac{\dfrac{\dfrac{[f:\sigma\to\sigma]^2 \qquad \begin{array}{c} \dfrac{[f:\sigma\to\sigma]^2 \qquad \dfrac{[f:\sigma\to\sigma]^2 \quad [x:\sigma]^1}{fx:\sigma}}{f(fx):\sigma} \\ \vdots \\ f(f\cdots(fx)\cdots):\sigma \end{array}}{f(f\cdots(fx)\cdots):\sigma}}{\lambda x\cdot f(f\cdots(fx)\cdots):\sigma\to\sigma}\,1}{\lambda f\cdot\lambda x\cdot f(f\cdots(fx)\cdots):(\sigma\to\sigma)\to\sigma\to\sigma}\,2
$$

Dans la suite on considère que tous les entiers $\underline{n}$ ont ce dernier type qu'on abrégera ι, y compris $\underline{0}$ et $\underline{1}$.

4. Écrire le type de plus.

Correction: Bien lire le sujet : il n'était pas demandé d'arbre de preuve, ce que beaucoup ont courageusement essayé de faire. Bien entendu l'addition prend deux ι et renvoie un ι, i.e., $\iota\to\iota\to\iota$.

5. Faisons l'hypothèse de l'existence d'une fonction fois pour la multiplication. Quel est son type ?

Correction: Comme pour l'addition : $\iota\to\iota\to\iota$. C'est bien de dire "comme l'addition", mais parfois c'est trop mal dit pour être accepté. Par exemple : "puisque la multiplication est une suite d'additions" n'est pas acceptable.
Deux personnes (SU et JM) m'ont proposé une définition de fois, et c'était juste. Je vous laisse analyser les deux réponses suivantes, équivalentes.

$$
\begin{array}{rcl}
\text{fois} & := & \lambda m\cdot\lambda n\cdot\lambda f\cdot m(nf)\\
\text{fois} & := & \lambda m\cdot\lambda n\cdot m(\text{plus }n)\underline{0}
\end{array}
$$

3 Déduction Naturelle Intuitionniste

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

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

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

1. Prouver que $(A\Rightarrow A)\Rightarrow A\Rightarrow A$. Qu'est-ce que ça vous rappelle, et pourquoi ce n'est pas un simple hasard ?

Barème:

1 Preuve correcte
1 Avec les décharges
1 Reconnaître les types de $\underline{n}$ par Curry-Howard
1 Plus spécifiquement celui de $\underline{1}$

Correction:

$$\dfrac{\dfrac{\dfrac{[A]^2 \quad [A \Rightarrow A]^1}{A}\Rightarrow\mathcal{E}}{A \Rightarrow A}\Rightarrow\mathcal{I}_2}{(A \Rightarrow A) \Rightarrow A \Rightarrow A}\Rightarrow\mathcal{I}_1$$

Beaucoup ont dit que ça rappellait le type des entiers de Church. Plus précisément c'est le type de $\underline{1}$ qu'il rappelle, même si le type de ce dernier est plus général. Mais il est important de prendre ce nombre, car c'est le seul pour lequel la correspondance de Curry-Howard s'applique. Et c'était ça qu'il fallait reconnaître.

Best-of:

- Ça rappelle le typage du premier exercice. Ce n'est pas un hasard, puisqu'on est dans le même partiel.
- Ça rappelle que $\Rightarrow$ est différent de $\vdash$.
- Ça me rappelle $A \Rightarrow A$, et ce n'est pas un simple hasard car c'est de la même forme.
- Ça ne me rappelle rien, ce n'est pas un simple hasard suite au [pot d'hier].
- Ça me rappelle un exemple du cours. Ce n'est pas un simple hasard car il était plus simple de reprendre un exo de partiel pour illustrer le cours.

2. Prouver $A \Rightarrow B, B \Rightarrow C \vdash A \Rightarrow (B \wedge C)$.

Correction:

$$\dfrac{\dfrac{\dfrac{[A]^1 \quad A \Rightarrow B}{B}\Rightarrow\mathcal{E} \qquad \dfrac{\dfrac{[A]^1 \quad A \Rightarrow B}{B}\Rightarrow\mathcal{E} \qquad B \Rightarrow C}{C}\Rightarrow\mathcal{E}}{B \wedge C}\wedge\mathcal{I}}{A \Rightarrow (B \wedge C)}\Rightarrow\mathcal{I}_1$$

3. Montrer que $A \vee B, \neg B \vdash A$, en utilisant la négation intuitionniste.

Correction: On rappelle que $\neg B := B \Rightarrow \bot$.

$$\dfrac{A \vee B \qquad [A]^1 \qquad \dfrac{\dfrac{[B]^2 \quad B \Rightarrow \bot}{\bot}\Rightarrow\mathcal{E}}{A}\bot\mathcal{E}}{A}\vee\mathcal{E}_1$$

4 Calcul des Séquents Classique

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

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

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

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

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

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

Best-of: Là, je sèche.

1. Prouver que pour toute formule F, on a $F \vdash F$.

Correction: Je vous l'accorde, ma question était mal posée, surtout si vous n'avez pas suivi avec attention le cours où j'insistais sur le fait que l'axiome porte sur une formule atomique, et que je distingue (parfois) A de F. Mais le formulaire ne répond même pas à ce critère...
Il s'agissait donc de faire une induction sur le connecteur le plus haut de la formule F:
$F = A$ (une formule atomique). Établi par l'axiome.

$F = G \wedge H$ Par induction on suppose que $G \vdash G$ et $H \vdash H$ et on montre que $F \vdash F$:

$$\cfrac{\cfrac{G \vdash G \qquad H \vdash H}{G, G \vdash H \wedge H} \vdash\wedge}{G \wedge G \vdash H \wedge H} \wedge\vdash$$

... Et continuer ainsi pour tous les connecteurs.

Best-of:

- Supposons $F \vdash \neg F$.

$$\dfrac{\dfrac{F \vdash \neg F}{F, F \vdash}\,\neg\vdash}{F \vdash}\,C\vdash$$

  Il y a donc une contradiction. Donc $\forall F, F \vdash F$.

- Sérieux, c'est évident quoi :-D. À part faire une méga disjonction sur toutes les natures possibles de l'opération racine de F et montrer que dans tous les cas ça remonte bien à l'étage du dessus et conclure par récurrence, je ne vois pas...

- $$\dfrac{\dfrac{\dfrac{}{\vdash \bot}}{F \vdash \bot}\,W\vdash}{F \vdash F(F \vee \bot = F)}\,\vdash W$$

- L'un des étudiants m'a numéroté toutes les règles sur le sujet, et a utilisé ces/ses numéros pour faire référence aux règles. De plus, plutôt que de faire des arbres de preuve, il rédigeait.

- Par l'absurde: on suppose qu'il existe une formule F tel que en ayant F en hypothèse on ne puisse pas théser F. C'est absurde car on ne peut pas conclure quelque chose que l'on suppose !

2. Prouver $(F \wedge G) \Rightarrow H \vdash (F \Rightarrow H) \vee (G \Rightarrow H)$.

Correction:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{F \vdash F} \quad \dfrac{}{G \vdash G}}{F, G \vdash F \wedge G}\,\wedge\vdash \qquad \dfrac{}{H \vdash H}}{F, G, (F \wedge G) \Rightarrow H \vdash H}\,\Rightarrow\vdash}{F, G, (F \wedge G) \Rightarrow H \vdash H, H}\,\vdash W}{F, (F \wedge G) \Rightarrow H \vdash H, G \Rightarrow H}\,\vdash\Rightarrow}{(F \wedge G) \Rightarrow H \vdash F \Rightarrow H, G \Rightarrow H}\,\vdash\Rightarrow}{(F \wedge G) \Rightarrow H \vdash (F \Rightarrow H) \vee (G \Rightarrow H), G \Rightarrow H}\,\vdash r\vee}{(F \wedge G) \Rightarrow H \vdash (F \Rightarrow H) \vee (G \Rightarrow H), (F \Rightarrow H) \vee (G \Rightarrow H)}\,\vdash l\vee}{(F \wedge G) \Rightarrow H \vdash (F \Rightarrow H) \vee (G \Rightarrow H)}\,\vdash C$$

Best-of: [Une longue preuve qui commence par l'"axiome" $G \vdash F$]...ce qui est faux car $G \vdash F$ est faux.

3. Que pensez-vous de l'affirmation suivante, portant sur les points (x, y) du plan:

$$(x = 0 \Rightarrow (x, y) = (0, 0)) \vee (y = 0 \Rightarrow (x, y) = (0, 0))$$

Best-of: On parle d'une ~~droite~~ courbe passant à l'origine.
La formule est vraie si $(x = 0 \wedge y = 0) \Rightarrow (x, y) = (0, 0)$.
Ceci est vrai dans le cadre d'un plan en 2 dimensions.
L'affirmation implique que x soit proportionelle à y, donc on a $x = \alpha y$ avec $\alpha \in \mathbb{R}$.
Cette affirmation est fausse, même si sa démonstration peut être exacte en logique classique. La faute au tiers exclu.
x et y sont lié [sic]. et pour ce qui est de l'affirmation je la trouve intéressante...
[Après une explication parfaitement satisfaisante, très convaincainte:] C'est là que $\Rightarrow$ diffère de $\wedge$.

5 À propos de ce cours

Bien entendu je m'engage à ne pas tenir compte des renseignements ci-dessous pour noter votre copie. 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.

Vous pouvez cocher plusieurs réponses par question.

1. Identité

   Option:

   Nom:

2. Assiduité

   a Jamais venu

   b Presque jamais venu

   c Souvent venu

   d Toujours présent

3. Travail personnel

   a Rien

   b Bachotage récent

   c Relu les notes entre chaque cours

   d Fait les anales

   e Lu d'autres sources

4. 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

5. 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

Best-of:

- Je le recommande, mais pas à tout le monde :-)
- (Il faudra que je sois plus clair à l'avenir.) J'ai du mal à comprendre à quoi il me servirait.

6. 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

Best-of:

- De bonnes remarques :
  - Comment on utilise cette théorie ?
  - Les CSI m'ont parlé d'un programme qui fait des preuves, comme ça marche ?
  - Ça veut dire quoi "prouver un algorithme" ?
- Enseignant pédagogue, mais cours absolument pas en phase avec les attentes des étudiants SCIA.

a bien du courage de faire ce cours.

est drôle.