DEA de Mathématiques et Fondements de l'Informatique

Exo 1. Pour chaque entier n on note $\bar{n}$ l'entier de Church

$$\bar{n} = \lambda f.\lambda x.\underbrace{(f)\ldots(f)}_{n\times}x.$$

On note S le terme réalisant le successeur sur les entiers de Church (que l'on écrira et que l'on typera dans le système F), φ le terme

$$\varphi = \lambda n.\lambda f.(((n)\lambda h.\lambda x.(h)(S)x)f)\bar{0}$$

- Soit o une variable de type de F. Montrer que φ est typable dans F du type :

$$\mathbb{N}^* \to (\mathbb{N} \to o) \to o$$

où $\mathbb{N} = \forall\alpha((\alpha \to \alpha) \to \alpha \to \alpha)$ est le type des entiers de Church
et $\mathbb{N}^* = \forall\alpha(((\alpha \to o) \to \alpha \to o) \to (\alpha \to o) \to \alpha \to o)$ est $\mathbb{N}$ dans lequel on a remplacé α par $\alpha \to o$.

Correction : Le successeur est évidemment typable de type $\mathbb{N} \to \mathbb{N}$. On pose $h : \mathbb{N} \to o$ et $x : \mathbb{N}$ si bien que $\varphi_0 = \lambda h.\lambda x.(h)(S)x$ devient de type $(\mathbb{N} \to o) \to \mathbb{N} \to o$. On pose $f : \mathbb{N} \to o$ et $n : \mathbb{N}^*$ si bien que par la règle de $\forall$-élim, $n : ((\mathbb{N} \to o) \to \mathbb{N} \to o) \to (\mathbb{N} \to o) \to \mathbb{N} \to o$. Comme $\bar{0}$ est de type $\mathbb{N}$, on a finalement $(((n)\varphi_0)f)\bar{0}$ de type o soit, par deux règles de $\to$-intro le résultat cherché.

- Effectuer la réduction de tête des termes $(\varphi)\bar{0}$, $(\varphi)\bar{1}$, $(\varphi)\bar{2}$. Plus généralement quelle sera la forme normale de tête obtenue par réduction de tête de $(\varphi)\bar{n}$ pour un entier n quelconque ?

Correction : La réduction de tête est la stratégie qui réduit le redex de tête à chaque étape, s'il y en a un. On rappelle qu'un λ-terme a obligatoirement la forme $\lambda\vec{x}.(U)U_1\ldots U_n$ où U est soit un redex (et dans ce cas c'est le redex de tête), soit une variable (auquel cas le terme est en forme normale de tête). On note φ_0 le terme $\lambda h.\lambda x.(h)(S)x$ si bien que $\varphi = \lambda n.\lambda f.(((n)\varphi_0)f)\bar{0}$. La réduction de tête de $(\varphi)\bar{0}$ donne :

$$\begin{aligned}(\varphi)\bar{0} &\to_{\beta_T} \lambda f.(((\lambda g.\lambda y.y)\varphi_0)f)\bar{0}\\ &\to_{\beta_T} \lambda f.((\lambda y.y)f)\bar{0}\\ &\to_{\beta_T} \lambda f.(f)\bar{0}\end{aligned}$$

Ce dernier terme est la forme normale de tête recherchée (remarquons que dans ce cas il s'agit même d'une forme normale puisque $\bar{0}$ est en forme normale).
La réduction de tête de $(\varphi)\bar{1}$ donne :

$$\begin{aligned}(\varphi)\bar{1} &\to_{\beta_T} \lambda f.(((\lambda g.\lambda y.(g)y)\varphi_0)f)\bar{0}\\ &\to_{\beta_T} \lambda f.((\lambda y.(\varphi_0)y)f)\bar{0}\\ &\to_{\beta_T} \lambda f.((\varphi_0)f)\bar{0} = \lambda f.((\lambda h.\lambda x.(h)(S)x)f)\bar{0}\\ &\to_{\beta_T} \lambda f.(\lambda x.(f)(S)x)\bar{0}\\ &\to_{\beta_T} \lambda f.(f)(S)\bar{0}\end{aligned}$$

Il n'y a plus de redex de tête mais la forme normale de tête obtenue n'est pas normale puisqu'elle contient le redex $(S)\bar{0}$.
La réduction de tête de $(\varphi)\bar{2}$ donne :

$$\begin{array}{lll}
(\varphi)\bar{2} & \rightarrow_{\beta_T} & \lambda f.(((\lambda g.\lambda y.(g)(g)y)\varphi_0)f)\bar{0} \\
& \rightarrow_{\beta_T} & \lambda f.((\lambda y.(\varphi_0)(\varphi_0)y)f)\bar{0} \\
& \rightarrow_{\beta_T} & \lambda f.((\varphi_0)(\varphi_0)f)\bar{0} = \lambda f.((\lambda h.\lambda x.(h)(S)x)(\varphi_0)f)\bar{0} \\
& \rightarrow_{\beta_T} & \lambda f.(\lambda x.((\varphi_0)f)(S)x)\bar{0} \\
& \rightarrow_{\beta_T} & \lambda f.((\varphi_0)f)(S)\bar{0} = \lambda f.((\lambda h.\lambda x.(h)(S)x)f)(S)\bar{0} \\
& \rightarrow_{\beta_T} & \lambda f.(\lambda x.(f)(S)x)(S)\bar{0} \\
& \rightarrow_{\beta_T} & \lambda f.(f)(S)(S)\bar{0}
\end{array}$$

Il n'y a plus de redex de tête mais la forme normale de tête obtenue n'est pas normale puisqu'elle contient les redex de $(S)(S)\bar{0}$ (question à 100 sous, combien y a-t-il de redex ?).
Plus généralement la réduction de tête de $(\varphi)\bar{n}$ donne :

$$\begin{array}{lll}
(\varphi)\bar{n} & \rightarrow_{\beta_T} & \lambda f.(((\lambda g.\lambda y.(g)\ldots(g)y)\varphi_0)f)\bar{0} \\
& \rightarrow_{\beta_T} & \lambda f.((\lambda y.(\varphi_0)\ldots(\varphi_0)y)f)\bar{0} \\
& \rightarrow_{\beta_T} & \lambda f.(\underbrace{(\varphi_0)(\varphi_0)\ldots(\varphi_0)}_{n\times}f)\bar{0} = \lambda f.((\lambda h.\lambda x.(h)(S)x)\underbrace{(\varphi_0)\ldots(\varphi_0)}_{n-1\times}f)\bar{0} \\
& \rightarrow_{\beta_T} & \lambda f.(\lambda x.((\varphi_0)\ldots(\varphi_0)f)(S)x)\bar{0} \\
& \rightarrow_{\beta_T} & \lambda f.((\varphi_0)\ldots(\varphi_0)f)(S)\bar{0} \\
& \vdots & \\
& \rightarrow_{\beta_T} & \lambda f.(\underbrace{(\varphi_0)\ldots(\varphi_0)}_{n-i\times}f)\underbrace{(S)\ldots(S)}_{i\times}\bar{0} \\
& \vdots & \\
& \rightarrow_{\beta_T} & \lambda f.((\lambda h.\lambda x.(h)(S)x)f)\underbrace{(S)\ldots(S)}_{n-1\times}\bar{0} \\
& \rightarrow_{\beta_T} & \lambda f.(\lambda x.(f)(S)x)(S)\ldots(S)\bar{0} \\
& \rightarrow_{\beta_T} & \lambda f.(f)(S)(S)\ldots(S)\bar{0} = \lambda f.(f)\underbrace{(S)\ldots(S)}_{n\times}\bar{0}
\end{array}$$

Encore une fois, ce dernier terme, bien qu'en forme normale de tête est loin d'être en forme normale (question à $n \times 100$ sous, combien de redex ? (indication : la réponse est dans la question)).

Exo 2. On note Y le terme

$$Y = \lambda f.(\lambda x.(f)(x)x)\lambda x.(f)(x)x$$

• Montrer que Y satisfait l'équation $(Y)U \simeq_\beta (U)(Y)U$ (le symbole $\simeq_\beta$ représente la β-équivalence) où U représente un terme quelconque (c'est à cause de cette équation que Y est appelé *opérateur de point fixe*, vous voyez pourquoi ?). En déduire, étant donné un terme H, une solution F de l'équation

$$F \simeq_\beta (H)F$$

Correction : On a les deux séquences de réductions suivantes :

$$\begin{array}{lll} (Y)U & \to_\beta & (\lambda x.(U)(x)x)\lambda x.(U)(x)x \\ & \to_\beta & (U)(\lambda x.(U)(x)x)\lambda x.(U)(x)x \end{array}$$

et

$$\begin{array}{lll} (U)(Y)U & \to_\beta & (U)(\lambda x.(U)(x)x)\lambda x.(U)(x)x \end{array}$$

donc les deux termes $(Y)U$ et $(U)(Y)U$ ont un réduit commun, par conséquent ils sont β-équivalents. Remarquons qu'il est faux que $(Y)U$ se β-*réduise* en $(U)(Y)U$.

Une solution de $F \simeq_\beta (H)F$ est $F = (Y)H$.

- En utilisant ce qui précède donner un terme W réalisant l'instruction *while*, *i.e.*, tel que étant donné trois termes quelconques C, A et E,

$$\begin{array}{llll} (((W)C)A)E & \simeq_\beta & E & \text{si } (C)E \simeq_\beta \mathbf{V}, \\ (((W)C)A)E & \simeq_\beta & (((W)C)A)(A)E & \text{si } (C)E \simeq_\beta \mathbf{F} \end{array}$$

où $\mathbf{V}$ et $\mathbf{F}$ représentent les booléens de Church $\lambda x.\lambda y.x$ et $\lambda x.\lambda y.y$.

Correction : Si B est un booléen de Church alors on voit facilement que $(B)UV \simeq_\beta U$ si $B \simeq_\beta \mathbf{V}$ et $(B)UV \simeq_\beta V$ si $B \simeq_\beta \mathbf{F}$. Par suite le terme W cherché doit satisfaire l'équation :

$$(((W)C)A)E \simeq_\beta (((C)E)E)(((W)C)A)(A)E$$

Il suffit pour cela que W satisfasse l'équation :

$$W \simeq_\beta \lambda c.\lambda a.\lambda e.(((c)e)e)(((W)c)a)(a)e$$

soit, en posant $H = \lambda w.\lambda c.\lambda a.\lambda e.(((c)e)e)(((w)c)a)(a)e$, W doit satisfaire $W \simeq_\beta (H)W$. En vertu de la question précédente, une solution est donc $W = (Y)H$.

Exo 3. Soit T un ensemble et X l'ensemble des parties de T. On dit qu'une fonction $f : X \to X$ est *continue* si elle est croissante pour l'inclusion et si pour tout $\sigma \in T$ et tout $a \in X$, si $\sigma \in f(a)$ alors il existe a_0 fini inclus dans a tel que $\sigma \in f(a_0)$. On dit qu'une partie D de X est *filtrante* si elle est non vide et si pour tout $a, a' \in D$, il existe $b \in D$ contenant a et a'.

- Montrer qu'une fonction croissante $f : X \to X$ est continue ssi elle commute aux unions des parties filtrantes de X, *i.e.*, pour toute partie filtrante D on a $f(\bigcup D) = \bigcup\{f(a),\ a \in D\}$.

Correction : À toutes fins utiles on rappelle que la notation $\bigcup D$, où D est une famille d'ensembles, représente la réunion des éléments de cette famille, *i.e.*, $\bigcup D = \bigcup\{x,\ x \in D\}$.

En guise de préliminaire, on montre que si D est une partie filtrante de X alors tout sous-ensemble fini D_0 de D est borné dans D (*i.e.*, il existe a dans D tel que $\bigcup D_0 \subseteq a$. D filtrant signifie D non vide et tout sous-ensemble à deux éléments de D est borné dans D). La démonstration est par récurrence sur n, le nombre d'éléments de D_0. Si $n = 0$, *i.e.*, D_0 est vide alors comme $\bigcup \emptyset = \emptyset$, D est non vide et comme n'importe quel ensemble contient $\emptyset$, il y a bien un majorant de $\bigcup D_0$ dans D. Sinon $D_0 = D_1 \cup \{a\}$ où D_1 a $n-1$ éléments et $a \in D$. Par hypothèse de récurrence, D_1 est borné par un élément b de D (*i.e.*, $\bigcup D_1 \subseteq b$). Comme

D est filtrant a et b sont bornés dans D par un ensemble c qui est donc un majorant de D_0 dans D.

On montre d'abord que si f est continue alors elle commute aux unions filtrantes. Soit donc D une partie filtrante. En notant $f(D) = \{f(a),\ a \in D\}$, on veut montrer que $\bigcup f(D) = f(\bigcup D)$. Comme f est croissante on a $f(a) \subseteq f(\bigcup D)$ pour tout $a \in D$, donc $\bigcup f(D) \subseteq f(\bigcup D)$. Réciproquement, soit $\sigma \in f(\bigcup D)$. Comme f est continue il existe a_0 fini inclus dans $\bigcup D$ tel que $\sigma \in f(a_0)$. Pour chaque $\tau \in a_0$ il y a un ensemble $a_\tau \in D$ tel que $\tau \in a_\tau$ (si bien que $a_0 \subseteq \bigcup\{a_\tau,\ \tau \in a_0\}$). Comme a_0 est fini, l'ensemble des a_τ est fini donc, par le préliminaire, est borné par un ensemble $a \in D$. Par conséquent $a_0 \subseteq a \in D$. Par croissance de f, on obtient alors $\sigma \in f(a) \subseteq f(\bigcup D)$.

Supposons maintenant que f commute aux unions filtrantes et montrons que f est continue. Soient $a \in X$ et $\sigma \in f(a)$. Soit D l'ensemble des sous-ensembles finis de a. Il est clair que D est filtrant (en particulier D n'est pas vide car il contient au moins $\emptyset$) et que $\bigcup D = a$. Donc, comme $f(a) = f(\bigcup D) = \bigcup f(D)$ par hypothèse sur f, il existe $a_0 \in D$ tel que $\sigma \in f(a_0)$. Autrement dit il existe un sous-ensemble fini a_0 de a tel que $\sigma \in f(a_0)$.

- Soit f une fonction croissante de X dans X. Montrer que pour tous entiers n et p, si $n \leq p$ alors $f^n(\emptyset) \subseteq f^p(\emptyset)$. En déduire que l'ensemble $D(f) = \{f^n(\emptyset),\ n \in \mathbb{N}\}$ est une partie filtrante de X.

Correction : On a $\emptyset \subseteq f^{p-n}(\emptyset)$ et comme f est croissante on en déduit que $f^n(\emptyset) \subseteq f^p\emptyset$. Autrement dit l'ensemble $D(f)$ est totalement ordonné par l'inclusion. Il est donc filtrant puisque toute paire $\{f^n(\emptyset), f^p(\emptyset)\}$ est bornée par $f^{\sup\{n,p\}}(\emptyset)$.

- Soit $f : X \to X$ une fonction continue et $a_0 = \bigcup D(f)$. Montrer que $f(a_0) = a_0$. Montrer de plus que pour tout a appartenant à X, si $f(a) = a$ alors $a_0 \subseteq a$ (autrement dit toute fonction continue de X dans X admet un plus petit point fixe).

Correction : Par la première question, f commute aux unions filtrantes et on vient de voir que $D(f)$ est filtrante. Donc

$$\begin{aligned}
f(a_0) &= \bigcup f(\{f^n(\emptyset),\ n \in \mathbb{N}\}) \\
&= \bigcup\{f^{n+1}(\emptyset),\ n \in \mathbb{N}\} \\
&= \emptyset \cup \bigcup\{f^{n+1}(\emptyset),\ n \in \mathbb{N}\} \\
&= \bigcup\{f^n(\emptyset),\ n \in \mathbb{N}\} \\
&= a_0
\end{aligned}$$

Soit maintenant a un point fixe de f. On a $\emptyset \subseteq a$, donc par croissance de f, pour tout $n \in \mathbb{N}$, $f^n(\emptyset) \subseteq f^n(a) = a$. Conséquemment $a_0 = \bigcup\{f^n(\emptyset),\ n \in \mathbb{N}\} \subseteq a$.

Exo 4. On se place dans la déduction naturelle pour le fragment intuititionniste minimal (le seul connecteur est l'implication) et on se donne deux formules atomiques σ et τ. Montrer que la formule de Pierce $((\sigma \to \tau) \to \sigma) \to \sigma$ n'est pas dérivable dans ce système.

Indication : voici le début de la preuve. D'après le théorème de normalisation on peut se restreindre à chercher une preuve normale, donc vérifiant la propriété de la sous-formule. la propriété de la sous-formule pour la déduction naturelle stipule que toute formule apparaissant dans une preuve normale doit être sous-formule de la conclusion ou des hypothèses. Pour le cas qui nous occupe on va donc montrer l'inexistence d'une preuve normale de $\mathcal{P} = ((\sigma \to \tau) \to \sigma) \to \sigma$ dont toutes les formules sont sous-formules de $\mathcal{P}$.

Pour montrer $\mathcal{P}$ sans hypothèse on a forcément utilisé une règle d'introduction ; en effet une élimination aurait une prémisse de la forme $A \to \mathcal{P}$ qui ne peut être sous-formule de $\mathcal{P}$. Donc on se ramène à trouver une preuve de σ sous l'hypothèse $\mathcal{P}_0 = (\sigma \to \tau) \to \sigma$. Une telle preuve ne peut se terminer par une intro puisque σ est atomique. Il s'agit donc d'une élim entre une formule de la forme $A \to \sigma$ et la formule A. Comme $A \to \sigma$ doit être une sous-formule de $\mathcal{P}$, il y a deux possibilités :

1. $A = \mathcal{P}_0$. Soit à trouver une preuve de $\mathcal{P}$ et une preuve de $\mathcal{P}_0$ sous l'hypothèse $\mathcal{P}_0$. Par le même raisonnement que précédemment la preuve de $\mathcal{P}$ ne peut se terminer que par une règle intro. Mais alors celle-ci se trouvant en position principale dans l'élim, on verrait apparaître un redex contredisant ainsi l'hypothèse de normalité de la preuve cherchée.
2. À vous de jouer...

Correction : ...La deuxième possibilité est $A = \sigma \to \tau$. Soit à trouver une preuve de $\mathcal{P}_0$ et une preuve de $\sigma \to \tau$ sous l'hypothèse $\mathcal{P}_0$. Comme $\mathcal{P}_0$ est évidemment prouvable sous l'hypothèse $\mathcal{P}_0$ il nous reste à trouver une preuve (normale et ne contenant que des sous-formules de $\mathcal{P}$) de $\sigma \to \tau$ sous l'hypothèse $\mathcal{P}_0$. Comme aucune sous-formule de $\mathcal{P}$ n'a la forme $A \to \sigma \to \tau$, une telle preuve ne peut se terminer que par une intro. Soit à démontrer τ sous les hypothèses $\mathcal{P}_0$ et σ. Un telle preuve se termine forcément par une élim entre une formule $A \to \tau$ et la formule A. La seule possibilité restant une sous-formule de $\mathcal{P}$ est $A = \sigma$. Soit à prouver σ sous l'hypothèse σ (ce qui ne pose pas vraiment de problème), et $\sigma \to \tau$ sous les hypothèses σ et $\mathcal{P}_0$. Une fois de plus par la contrainte de sous-formule une telle preuve ne peut se finir par une flèche élim. Donc elle se termine par une intro puisque $\sigma \to \tau$ n'est pas une des hypothèses. Mais alors on se retrouve avec un intro en position principale dans une élim, contredisant à nouveau la normalité de la preuve.