Examen Programmation I (2023-24)

Cet examen se déroule en deux parties. Ceci est la première partie ; elle n'est pas notée, mais il est indispensable de la faire pour pouvoir faire la deuxième partie, qui elle sera notée et en temps limité. Je donnerai un corrigé de la première partie peu avant la deuxième partie. La deuxième partie consistera en les questions dont l'énoncé est occulté par un $\ll [\ldots] \gg$; uniquement ces questions, pas les définitions, règles et résultats présentés en première partie. Lors de la deuxième partie, vous aurez donc besoin de l'énoncé de la première partie. Vous aurez aussi besoin de vos notes de cours, et de vos réponses à la première partie. Tous documents écrits autorisés. Pas d'ordinateur, de tablette, de smartphone.

On insistera sur la correction et la clarté des réponses.

Toute affirmation devra être justifiée explicitement, par un théorème du cours, par un numéro de question, par une référence à une règle.

N'inventez pas vos propres notations, et réutilisez les miennes, même si elles ne vous plaisent pas.

Je veux une copie au propre, pas un brouillon : pas de rature, notamment. L'orthographe, et plus généralement la présentation, est importante.

Je corrigerai vraisemblablement toutes les copies en corrigeant d'abord toutes les questions 1 de tout le monde, puis toutes les questions 2, et ainsi de suite : ne comptez pas sur le fait que je me souvienne de ce que vous avez écrit dans une question précédente.

Le sujet porte sur une extension de PCF avec des choix probabilistes. Mieux : nous aurons un type explicite $D\tau$ des distributions sur τ.

On note $\underline{\mathbb{I}}$ le dcpo $[0, 1]$ muni de son ordre usual $\leq$. Il sera pratique d'appeler *fonctionnelle* sur un dcpo X tout élément du dcpo $[[X \to \underline{\mathbb{I}}] \to \underline{\mathbb{I}}]$. Une *distribution* sur X est une fonctionnelle F sur X qui est *linéaire*, au sens où :

$$F(ah + bk) = aF(h) + bF(k) \tag{1}$$

pour toutes fonctions continues $h, k \in [X \to \underline{\mathbb{I}}]$, et pour tous $a, b \in \underline{\mathbb{I}}$ tels que $a + b \leq 1$. L'idée est que $F(h)$ est l'intégrale de h par rapport à une mesure ; nous n'aurons pas besoin de dire quelle mesure, et nous raisonnerons directement sur les fonctionnelles.

On note $\mathbf{D}(X)$ le sous-ensemble ordonné de $[[X \to \underline{\mathbb{I}}] \to \underline{\mathbb{I}}]$ formé des fonctionnelles linéaires sur X.

Question 1 [...]

▌ *[...]*

On en déduit le résultat suivant.

Lemme 1 *Pour tout dcpo X, $\mathbf{D}(X)$ est un dcpo, où les sups dirigés sont calculés point à point.*

Nous admettrons ce résultat.

Pour tout $x \in X$, on note δ_x la fonction qui à tout $h \in [X \to \underline{\mathbb{I}}]$ associe $h(x)$. Comme les sups dirigés sont calculés point à point dans $[X \to \underline{\mathbb{I}}]$, δ_x est Scott-continue. Il est clair que δ_x est linéaire, et c'est donc une distribution sur X. C'est la *distribution de Dirac en x.*

En général, toute distribution de la forme $\sum_{i=1}^n a_i \delta_{x_i}$, définie comme $h \in [X \to \underline{\mathbb{I}}] \mapsto \sum_{i=1}^n a_i h(x_i)$ (avec $n \in \mathbb{N}$, $a_1, \cdots, a_n \geq 0$, $\sum_{i=1}^n a_i \leq 1$, $x_1, \cdots, x_n \in X$ deux à deux distincts), est une distribution, représentant le choix aléatoire d'un élément x_i avec (sous-)probabilité a_i.

Question 2 [...]

▌ *[...]*

Pour tous dcpos X et Y, pour toute fonction Scott-continue $f \colon X \to \mathbf{D}(Y)$, on note $f^\dagger$ la fonction de $\mathbf{D}(X)$ vers $\mathbf{D}(Y)$ définie par :

$$f^\dagger(F)(k) \stackrel{\text{def}}{=} F(x \in X \mapsto f(x)(k)) \tag{2}$$

pour toute distribution $F \in \mathbf{D}(X)$, pour tout fonction Scott-continue $k \in [Y \to \underline{\mathbb{I}}]$. La notation $x \in X \mapsto \cdots$ désigne la fonction qui à tout $x \in X$ associe $\cdots$. On admettra le résultat suivant.

Lemme 2 *Pour tous dcpos X et Y, pour toute fonction $f \in [X \to \mathbf{D}(Y)]$, $f^\dagger$ est une fonction bien définie et Scott-continue de $\mathbf{D}(X)$ vers $\mathbf{D}(Y)$.*

Question 3 (∗) [...]

[...]

Question 4 (∗) Montrer l'égalité :

$$(g^\dagger \circ f)^\dagger = g^\dagger \circ f^\dagger, \tag{3}$$

pour toutes fonctions Scott-continues $f\colon X \to \mathbf{D}(Y)$ et $g\colon Y \to \mathbf{D}(Z)$, où X, Y et Z sont des dcpos quelconques. Vous utiliserez les notations : F pour un élément de $\mathbf{D}(X)$, h de $[[X \to \underline{\mathbb{I}}]$, k de $[Y \to \underline{\mathbb{I}}]$, ℓ de $[Z \to \underline{\mathbb{I}}]$, x de X, y de Y, z de Z.

Pour toute $F \in \mathbf{D}(X)$, pour toute $\ell \in [Z \to \underline{\mathbb{I}}]$,

$$\begin{aligned}(g^\dagger \circ f)^\dagger(F)(\ell) &= F(x \in X \mapsto (g^\dagger \circ f)(x)(\ell)) \\ &= F(x \in X \mapsto g^\dagger(f(x))(\ell)) \\ &= F(x \in X \mapsto f(x)(y \in Y \mapsto g(y)(\ell))),\end{aligned}$$

et

$$\begin{aligned}g^\dagger(f^\dagger(F))(\ell) &= f^\dagger(F)(y \in Y \mapsto g(y)(\ell)) \\ &= F(x \in X \mapsto f(x)(y \in Y \mapsto g(y)(\ell))).\end{aligned}$$

On admettra que les égalités suivantes sont elles aussi valides :

$$\eta_X^\dagger = \mathrm{id}_{\mathbf{D}X} \tag{4}$$

$$f^\dagger \circ \eta_X = f \qquad (f \in [X \to \mathbf{D}(Y)]). \tag{5}$$

Ceci énonce que $(\mathbf{D}, \eta, \_^\dagger)$ est une *monade*, si vous êtes curieux.

Les types sont :

$$\begin{aligned}\sigma, \tau, \cdots ::= {} & \texttt{int} && \text{entiers} \\ | \ & \sigma \to \tau && \text{functions} \\ | \ & D\tau && \text{distributions (nouveau).}\end{aligned}$$

La sémantique dénotationnelle des types est donnée par :

— $[\![\texttt{int}]\!] = \mathbb{Z}_\perp$; $\mathbb{Z}$ est ordonné par $=$, et $\mathbb{Z}_\perp$ est donc plat.

— $[\![\sigma \to \tau]\!] = [[\![\sigma]\!] \to [\![\tau]\!]]$.

— $[\![D\tau]\!] \stackrel{\text{def}}{=} \mathbf{D}([\![\tau]\!])$ (nouveau).

Question 5 [...]

$$\frac{}{\vdash x_\tau : \tau} \qquad \frac{}{\vdash \dot{n} : \texttt{int}} \qquad \frac{\vdash u : \sigma \quad \vdash v : \tau}{\vdash \texttt{let}\ x_\sigma = u\ \texttt{in}\ v : \tau}$$

$$\frac{\vdash u : \sigma \to \tau \quad \vdash v : \sigma}{\vdash uv : \tau} \qquad \frac{\vdash u : \tau}{\vdash \texttt{fn}\, x_\sigma.u : \sigma \to \tau} \qquad \frac{\vdash u : \tau \to \tau}{\vdash \texttt{rec}\, u : \tau}$$

$$\frac{\vdash u : \texttt{int} \quad \vdash v : \texttt{int}}{\vdash u \dot{+} v : \texttt{int}} \qquad \frac{\vdash u : \texttt{int}}{\vdash \dot{-} u : \texttt{int}} \qquad \frac{\vdash u : \texttt{int} \quad \vdash v : \tau \quad \vdash w : \tau}{\vdash \texttt{if}\, u = 0\, \texttt{then}\, v\ \texttt{else}\ w : \tau}$$

$$\frac{\vdash u : \tau}{\vdash \texttt{ret}_\tau\, u : D\tau} \qquad \frac{\vdash u : D\sigma \quad \vdash v : D\tau}{\vdash \texttt{do}\, x_\sigma \leftarrow u; v\ : D\tau} \qquad \frac{\vdash u : D\tau \quad \vdash v : D\tau}{\vdash u \oplus v : D\tau}$$

FIGURE 1 – Les expressions de PCF+distributions avec leurs types

Question 6 [...]

[...]

Les expressions de PCF+distributions sont définies comme pour PCF, avec en plus des constructions $\texttt{ret}_\tau\, u$ (distribution retournant toujours $u : \tau$), $\texttt{do}\, x_\sigma \leftarrow u; v$ (≪ échantillonner x_σ selon la distribution u puis exécuter v ≫) et $u \oplus v$ (≪ effectuer u ou v avec probabilité $1/2$ ≫). La grammaire complète, avec les contraintes de typage, est donnée à la figure 1 ; x_τ parcourt un ensemble infini dénombrable de variables de type τ, pour chaque type τ, et il y a autant de constantes $\dot{n}$ que d'entiers $n \in \mathbb{Z}$. La syntaxe des fonctions change par rapport à la version de PCF vue en cours : on a une construction $\texttt{fn}\, x_\sigma.u$ (≪ fonction qui à x_σ associe la valeur de u ≫, qui aurait été écrite $\texttt{letrec}\ f_{\sigma\to\tau}(x_\sigma) = u\ \texttt{in}\ f$, avec f une variable fraîche, dans le cours), une construction `let` comme en pureML, et une construction de récursion `rec` (de sorte que l'ancienne construction $\texttt{letrec}\ f_{\sigma\to\tau}(x_\sigma) = u\ \texttt{in}\ v$ peut s'exprimer via $\texttt{let}\ f_{\sigma\to\tau} = \texttt{rec}(\texttt{fn}\, f_{\sigma\to\tau}.\texttt{fn}\, x_\sigma.u)\ \texttt{in}\ v$).

La sémantique dénotationnelle est donnée à la figure 2. Les environnements ρ sont des fonctions qui à toute variable x_σ (pour tout type σ) associe un élément $\rho(x_\sigma)$ de $[\![\sigma]\!]$. La notation $\frac{1}{2}F + \frac{1}{2}G$, pour F et G des distributions sur le même dcpo X, telle qu'utilisée dans la définition de $[\![u \oplus v]\!]\rho$, est la distribution $h \in [X \to \underline{\mathbb{I}}] \mapsto \frac{1}{2}F(h) + \frac{1}{2}G(h)$.

On admettra que, pour chaque terme u, si u est de type τ, alors $[\![u]\!]\rho$ est un élément de $[\![\tau]\!]$.

$$\llbracket x_\tau \rrbracket\rho \stackrel{\text{def}}{=} \rho(x_\tau) \quad \llbracket \dot{n} \rrbracket\rho \stackrel{\text{def}}{=} n \qquad \llbracket \texttt{let}\ x_\sigma = u\ \texttt{in}\ v \rrbracket\rho \stackrel{\text{def}}{=} \llbracket v \rrbracket(\rho[x_\sigma \mapsto \llbracket u \rrbracket\rho)$$

$$\llbracket uv \rrbracket\rho \stackrel{\text{def}}{=} \llbracket u \rrbracket\rho(\llbracket v \rrbracket\rho) \qquad \llbracket \texttt{fn}\, x_\sigma.u \rrbracket\rho \stackrel{\text{def}}{=} (V \in \llbracket\sigma\rrbracket \mapsto \llbracket u \rrbracket(\rho[x_\sigma \mapsto V]))$$

$$\llbracket \texttt{rec}\, u \rrbracket\rho \stackrel{\text{def}}{=} \mathrm{lfp}(\llbracket u \rrbracket\rho) \qquad \llbracket \dot{-}u \rrbracket\rho \stackrel{\text{def}}{=} \begin{cases} -\llbracket u \rrbracket\rho & \text{si } \llbracket u \rrbracket\rho \neq \bot \\ \bot & \text{sinon} \end{cases}$$

$$\llbracket u \dot{+} v \rrbracket\rho \stackrel{\text{def}}{=} \begin{cases} \llbracket u \rrbracket\rho + \llbracket v \rrbracket\rho & \text{si } \llbracket u \rrbracket\rho \neq \bot, \llbracket v \rrbracket\rho \neq \bot \\ \bot & \text{sinon} \end{cases}$$

$$\llbracket \texttt{if}\ u = 0\ \texttt{then}\ v\ \ \texttt{else}\ \ w \rrbracket\rho \stackrel{\text{def}}{=} \begin{cases} \llbracket v \rrbracket\rho & \text{si } \llbracket u \rrbracket\rho = 0 \\ \llbracket w \rrbracket\rho & \text{si } \llbracket u \rrbracket\rho \neq \bot, 0 \\ \bot & \text{si } \llbracket u \rrbracket\rho = \bot \end{cases}$$

$$\llbracket \texttt{ret}_\tau\, u \rrbracket\rho \stackrel{\text{def}}{=} \delta_{\llbracket u \rrbracket\rho} \qquad \llbracket \texttt{do}\, x_\sigma \leftarrow u; v \rrbracket\rho \stackrel{\text{def}}{=} (V \in \llbracket\Sigma\rrbracket \mapsto \llbracket v \rrbracket(\rho[x_\sigma \mapsto V])^\dagger(\llbracket u \rrbracket\rho)$$

$$\llbracket u \oplus v \rrbracket\rho \stackrel{\text{def}}{=} \tfrac{1}{2}\llbracket u \rrbracket\rho + \tfrac{1}{2}\llbracket v \rrbracket\rho$$

FIGURE 2 – Sémantique dénotationnelle

Question 7 [...]

[...]

Question 8 (∗) L'intérêt de la construction `rec` est que l'on peut définir bien d'autres choses que des fonctions par récursion. À titre d'exemple :

(a) Quels sont les points fixes de la fonction $F \in \mathbf{D}(\mathbb{Z}_\perp) \mapsto (h \in [\mathbb{Z}_\perp \to \underline{\mathbb{I}}] \mapsto \frac{1}{4}(h(1) + h(2) + h(3) + F(h))$?

(b) En déduire la valeur de

$$\llbracket \texttt{rec}(\texttt{fn}\, r_{D\texttt{int}}.(\texttt{ret}_{\texttt{int}}\, \dot{1} \oplus \texttt{ret}_{\texttt{int}}\, \dot{2}) \oplus (\texttt{ret}_{\texttt{int}}\, \dot{3} \oplus r_{D\texttt{int}})) \rrbracket\rho,$$

où ρ est un environnement arbitraire.

(a) Les points fixes en question sont les distributions F telles que pour toute $h \in [\mathbb{Z}_\perp \to \underline{\mathbb{I}}]$, $F(h) = \frac{1}{4}(h(1) + h(2) + h(3) + F(h))$, autrement dit $F(h) = \frac{1}{3}(h(1) + h(2) + h(3))$. Il n'y a donc qu'une solution, et c'est $\frac{1}{3}(\delta_1 + \delta_2 + \delta_3)$.
(b) Eh bien, $\frac{1}{3}(\delta_1 + \delta_2 + \delta_3)$, justement, le choix aléatoire uniforme parmi 1, 2, 3.

La sémantique opérationnelle (à petits pas) se trouve en figure 3. Ses configurations s, t, ... sont de la forme $u \cdot C$, où $u \colon \sigma$ et C est un *contexte* (d'exécution) de type $\sigma \Rightarrow \lambda$ (où σ et λ sont deux types arbitraires, mais σ

$$uv \cdot C \xrightarrow{1} u \cdot \bullet\, v \cdot C \quad (app?) \qquad (\mathtt{fn}\, x_\sigma.u) \cdot \bullet\, v \cdot C \xrightarrow{1} u[x_\sigma := v] \cdot C \quad (app!)$$

$$\mathtt{let}\ x_\sigma = u\ \mathtt{in}\ v \cdot C \xrightarrow{1} v[x_\sigma := u] \cdot C \quad (\mathtt{let})$$

$$\mathtt{rec}\, u \cdot C \xrightarrow{1} u(\mathtt{rec}\, u) \cdot C \quad (\mathtt{rec})$$

$$\dot{-}u \cdot C \xrightarrow{1} u \cdot \dot{-} \bullet \cdot C \quad (\dot{-}?) \qquad \dot{n} \cdot \dot{-} \bullet \cdot C \xrightarrow{1} \dot{\overline{-n}} \cdot C \quad (\dot{-}!)$$

$$u \dot{+} v \cdot C \xrightarrow{1} u \cdot \bullet \dot{+} v \cdot C \quad (\dot{+}?_1) \qquad \dot{m} \cdot \bullet \dot{+} v \cdot C \xrightarrow{1} v \cdot \dot{m} \dot{+} \bullet \cdot C \quad (\dot{+}?_2)$$

$$\dot{n} \cdot \dot{m} \dot{+} \bullet \cdot C \xrightarrow{1} \dot{\overline{m+n}} \cdot C$$

$$\mathtt{if}\, u = 0\ \mathtt{then}\ v\ \ \mathtt{else}\ \ w \cdot C \xrightarrow{1} u \cdot \mathtt{if} \bullet = 0\ \mathtt{then}\ v\ \ \mathtt{else}\ \ w \cdot C \quad (\mathtt{if}?)$$

$$\dot{0} \cdot \mathtt{if} \bullet = 0\ \mathtt{then}\ v\ \ \mathtt{else}\ \ w \cdot C \xrightarrow{1} v \cdot C \quad (\mathtt{if}!_{=0})$$

$$\dot{n} \cdot \mathtt{if} \bullet = 0\ \mathtt{then}\ v\ \ \mathtt{else}\ \ w \cdot C \xrightarrow{1} w \cdot C \quad \text{si } n \neq 0 \quad (\mathtt{if}!_{\neq 0})$$

$$\mathtt{do}\, x_\sigma \leftarrow u; v \cdot C \xrightarrow{1} u \cdot \mathtt{do}\, x_\sigma \leftarrow \bullet; v \cdot C \quad (\mathtt{do}?)$$

$$\mathtt{ret}_\sigma\, u \cdot \mathtt{do}\, x_\sigma \leftarrow \bullet; v \cdot C \xrightarrow{1} v[x_\sigma := u] \cdot C \quad (\mathtt{do}!)$$

$$u \oplus v \cdot C \xrightarrow{1/2} u \cdot C \quad (\oplus_1) \qquad u \oplus v \cdot C \xrightarrow{1/2} v \cdot C \quad (\oplus_2)$$

$$\mathtt{ret}_\tau\, u \cdot \epsilon \xrightarrow{1} u \cdot \mathtt{ret}_\tau \bullet \quad (\mathtt{ret})$$

FIGURE 3 – Sémantique opérationnelle

est le même pour u et pour C) ; dans ces conditions, le *type* de $u \cdot C$ est λ. Les contextes et leurs typages sont définis par :

$$\frac{}{\vdash \epsilon\colon \lambda \Rightarrow \lambda} \qquad \frac{}{\vdash \mathtt{ret}_\tau \bullet\colon \tau \Rightarrow D\tau}$$

$$\frac{\vdash C\colon D\tau \Rightarrow \lambda}{\vdash \mathtt{do}\, x_\sigma \leftarrow \bullet; v \cdot C\colon D\sigma \Rightarrow \lambda} \qquad \frac{\vdash C\colon \tau \Rightarrow \lambda \quad \vdash v\colon \sigma}{\vdash \bullet\, v\colon (\sigma \to \tau) \cdot C \Rightarrow \lambda} \qquad \frac{\vdash C\colon \mathtt{int} \Rightarrow \lambda}{\vdash \dot{-} \bullet \cdot C\colon \mathtt{int} \Rightarrow \lambda}$$

$$\frac{\vdash C\colon \mathtt{int} \Rightarrow \lambda \quad \vdash v\colon \mathtt{int}}{\vdash \bullet \dot{+} v \cdot C\colon \mathtt{int} \Rightarrow \lambda} \qquad \frac{\vdash C\colon \mathtt{int} \Rightarrow \lambda}{\vdash \dot{m} \dot{+} \bullet \cdot C\colon \mathtt{int} \Rightarrow \lambda} \qquad \frac{\vdash C\colon \tau \Rightarrow \lambda \quad \vdash v\colon \tau \quad \vdash w\colon \tau}{\vdash \mathtt{if} \bullet = 0\ \mathtt{then}\ v\ \ \mathtt{else}\ \ w \cdot C\colon \mathtt{int} \Rightarrow \lambda}$$

L'idée est que $\bullet$ représente un trou, dans lequel on mettra une valeur une fois calculée. Par exemple, dans $u \cdot \bullet v \cdot C$ (voir la règle ($app?$)), l'idée est que l'on va chercher à calculer u, et qu'une fois trouvée sa valeur (une fonction, normalement), on l'appliquera à v ; une fois le résultat de uv obtenu, on poursuivra le calcul avec C, etc. La notation $u[x_\sigma := v]$ opère une forme de remplacement de x_σ par v dans u. On n'aura pas à connaître sa définition

explicite, juste que :

$$[\![u[x_\sigma := v]]\!]\rho = [\![u]\!](\rho[x_\sigma \mapsto [\![v]\!]\rho]). \tag{6}$$

Les règles de sémantique opérationnelle définissent des relations $\xrightarrow{a}$, $a \in [0,1]$. Pour deux configurations s et t, $s \xrightarrow{a} t$ se lit « on peut aller de s à t en une étape, avec probabilité a ». Une *trace* est une suite de la forme :

$$s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} \cdots \xrightarrow{a_k} s_k$$

et il s'agit d'une trace *de* s_0 *à* s_k, de *longueur* k, et de *probabilité* $a \stackrel{\text{def}}{=} a_1.a_2 \cdots a_k$, ce que l'on notera en abrégé $s_0 \xrightarrow{a}{}^{k} s_k$, où $s_0 \xrightarrow{a}{}^{*} s_k$ si l'on ne souhaite pas mentionner la longueur k. On note :

$$\Pr[s \downarrow^{\leq K} n] \stackrel{\text{def}}{=} \sum_{k=0}^{K} \sum_{s \xrightarrow{a}{}^{k} \dot{n}\cdot \mathtt{ret}_{\mathtt{int}}\, \bullet} a$$

la somme des probabilités de toutes les traces de longueur au plus K ($K \in \mathbb{N}$) de s à la configuration $\dot{n} \cdot \mathtt{ret}_{\mathtt{int}}\, \bullet$, où $n \in \mathbb{N}$. Ceci n'a de sens que pour une configuration s de type $D\mathtt{int}$. On note aussi :

$$\Pr[s \downarrow n] \stackrel{\text{def}}{=} \sup_{K \in \mathbb{N}} \Pr[s \downarrow^{\leq K} n],$$

il s'agit de la (sous-)probabilité que s calcule n *opérationnellement*.

On définit la sémantique dénotationnelle $[\![C]\!]\rho$ d'un contexte C par récurrence sur C, comme suit.

$$[\![\epsilon]\!]\rho \stackrel{\text{def}}{=} \mathrm{id} \qquad [\![\mathtt{ret}_\tau\, \bullet]\!]\rho \stackrel{\text{def}}{=} \eta_{[\![\tau]\!]}$$

$$[\![\mathtt{do}\, x_\sigma \leftarrow \bullet; v \cdot C]\!]\rho \stackrel{\text{def}}{=} [\![C]\!]\rho \circ (V \in [\![\sigma]\!] \mapsto [\![v]\!](\rho[x_\sigma \mapsto V]))^\dagger$$

$$[\![\bullet v \cdot C]\!]\rho \stackrel{\text{def}}{=} [\![C]\!]\rho \circ (f \in [\![\sigma \to \tau]\!] \mapsto f([\![v]\!]\rho))$$

$$[\![\dot{-}\, \bullet \cdot C]\!]\rho \stackrel{\text{def}}{=} [\![C]\!]\rho \circ (n \in \mathbb{Z}_\perp \mapsto \begin{cases} -n & \text{si } n \neq \perp \\ \perp & \text{sinon} \end{cases})$$

$$[\![\bullet \dot{+} v \cdot C]\!]\rho \stackrel{\text{def}}{=} [\![C]\!]\rho \circ (m \in \mathbb{Z}_\perp \mapsto \begin{cases} \perp & \text{si } m = \perp \text{ ou } [\![v]\!]\rho = \perp \\ m + [\![v]\!]\rho & \text{sinon} \end{cases})$$

$$[\![\dot{m} \dot{+} \bullet \cdot C]\!]\rho \stackrel{\text{def}}{=} [\![C]\!]\rho \circ (n \in \mathbb{Z}_\perp \mapsto \begin{cases} \perp & \text{si } n = \perp \\ m + n & \text{sinon} \end{cases})$$

$$[\![\mathtt{if}\, \bullet = 0\, \mathtt{then}\, v\ \mathtt{else}\ w \cdot C]\!]\rho \stackrel{\text{def}}{=} [\![C]\!]\rho \circ (n \in \mathbb{Z}_\perp \mapsto \begin{cases} [\![v]\!]\rho & \text{si } n = 0 \\ [\![w]\!]\rho & \text{si } n \neq \perp, 0 \\ \perp & \text{si } n = \perp \end{cases})$$

Ceci nous permet de définir la sémantique dénotationnelle $[\![s]\!]\rho$ d'une configuration s par :

$$[\![u \cdot C]\!]\rho \stackrel{\text{def}}{=} [\![C]\!]\rho([\![u]\!]\rho).$$

On appelle règles *déterministes* les règles de la forme $s \xrightarrow{1} t$ de la figure 3, autrement dit toutes sauf les règles $(\oplus_1)$ et $(\oplus_2)$.

Question 9 [...]

[...]

On peut démontrer de même que toutes les règles déterministes $s \xrightarrow{1} t$ sont correctes, au sens suivant.

Lemme 3 *Pour toute règle déterministe $s \xrightarrow{1} t$, pour tout environnement ρ, $[\![s]\!]\rho = [\![t]\!]\rho$.*

[...]

Question 10 (∗∗) Quelle est la forme générale des contextes C de type $D\tau \Rightarrow D\texttt{int}$? Le type τ est arbitraire.

Ce sont les contextes de la forme :

$$\texttt{do}\, x_{\sigma_1} \leftarrow \bullet; v_1 \cdot \texttt{do}\, x_{\sigma_2} \leftarrow \bullet; v_2 \cdot \cdots \cdot \texttt{do}\, x_{\sigma_n} \leftarrow \bullet; v_n \cdot \epsilon$$

où ϵ est de type $D\texttt{int} \Rightarrow D\texttt{int}$, où les termes v_1, ..., v_n sont de types appropriés.
En effet, si C est de la forme $E \cdot C'$, alors comme C est d'un type de la forme $D\tau \Rightarrow \cdots$, E est forcément de la form $\texttt{do}\, x_\sigma \leftarrow \bullet; v$, et alors C' est lui-même un contexte de type $D\tau' \Rightarrow \cdots$. On analyse C' de même, pour arriver à soit ϵ, soit $\texttt{ret}_{\texttt{int}}\, \bullet$; mais ce dernier est de type $\texttt{int} \Rightarrow D\texttt{int}$, qui n'est pas de la forme désirée.

Question 11 [...]

[...]

Question 12 [...]

[...]

Question 13 [...]

[. . .]

Nous nous attaquons maintenant à l'adéquation. Nous n'en ferons pas la preuve complète, mais nous allons en toucher quelques aspects. On définit des relations binaires R_τ et $R_\tau^\perp$ indexées par les types τ comme suit : R_τ est une relation entre termes de type τ et valeurs de $[\![\tau]\!]$, et $R_\tau^\perp$ est une relation entre contextes C de type $D\tau \Rightarrow D\mathtt{int}$ et fonctions $h \in [[\![\tau]\!] \to [\![D\mathtt{int}]\!]]$. Par commodité, nous dirons « pour touts $a\ R_\tau\ b$ » pour dire « pour tous a et b [dans les ensembles appropriés] tels que $a\ R_\tau\ b$ ».

— $u\ R_{\mathtt{int}}\ n$ si et seulement si $n = \perp$, ou bien $u \cdot \epsilon \xrightarrow{1}{}^{*} \dot{n} \cdot \epsilon$;

— $u\ R_{\sigma\to\tau}\ f$ si et seulement si pour tous $v\ R_\sigma\ a$, $uv\ R_\tau\ f(a)$;

— $u\ R_{D\tau}\ F$ si et seulement si pour tous $C\ R_\tau^\perp\ h$, pour tout $n \in \mathbb{Z}$, $\Pr[u \cdot C \downarrow n] \geq h^\dagger(F)(\mathbf{1}_n)$;

— $C\ R_\tau^\perp\ h$ si et seulement si pour tous $v\ R_\tau\ b$, pour tout $n \in \mathbb{Z}$, $\Pr[\mathtt{ret}_\tau\, v \cdot C \downarrow n] \geq h(b)(\mathbf{1}_n)$.

Un terme u *clos* si et seulement s'il n'a aucune variable libre (toutes ses variables sont liées, par un `fn`, par un `let`, ou par un `do`). Pour tout terme clos u de type τ, on définit l'ensemble $u\ R_\tau$ des valeurs $a \in [\![\tau]\!]$ telles que $u\ R_\tau\ a$.

Lemme 4 *Pour tout terme clos u de type τ, l'ensemble $u\ R_\tau$ contient $\perp_\tau$ et est clos par sups dirigés (i.e., pour toute famille dirigée $(a_i)_{i\in I}$ dans $u\ R_\tau$, $\sup_{i\in I} a_i$ est aussi dans $u\ R_\tau$).*

Démonstration. Par récurrence sur le type τ.

Lorsque $\tau = \mathtt{int}$, $u\ R_\tau$ est un ensemble égal soit à $\{\perp\}$ soit à $\{n, \perp\}$, où n est l'unique entier tel que $u \cdot \epsilon \xrightarrow{1}{}^{*} \dot{n} \cdot \epsilon$ s'il existe (les règles déterministes … sont déterministes). Ces deux ensembles contiennent $\perp_{\mathtt{int}} = \perp$, et toutes les familles dirigées incluses dans l'un ou dans l'autre ensemble sont triviales, au sens où elles contiennent déjà leur borne supérieure, donc $\{\perp\}$ et $\{n, \perp\}$ sont clos par sups dirigés.

Pour un type de la forme $\sigma \to \tau$, $u\ R_{\sigma\to\tau}$ est l'ensemble des fonctions $f \in [[\![\sigma]\!] \to [\![\tau]\!]]$ telles que pour tous $v\ R_\sigma\ a$, $uv\ R_\tau\ f(a)$. Cet ensemble contient $\perp_{\sigma\to\tau}$, puisque pour tous $v\ R_\sigma\ a$, $\perp_{\sigma\to\tau}(a) = \perp_\tau$, et $uv\ R_\tau\ \perp_\tau$ par hypothèse de récurrence. Pour toute famille dirigée $(f_i)_{i\in I}$ dans $u\ R_{\sigma\to\tau}$, de borne supérieure f (calculée point à point), on a que pour tous $v\ R_\sigma\ a$, pour tout $i \in I$, $uv\ R_\tau\ f_i(a)$. La famille $(f_i(a))_{i\in I}$ est dirigée, de borne supérieure égale à $f(a)$ (car les sups sont calculés point à point), donc $uv\ R_\tau\ f(a)$ par hypothèse de récurrence. On en déduit que $u\ R_{\sigma\to\tau}\ f$.

Question 14 [...]

[...]

Nous admettrons le lemme suivant.

Lemme 5 *Si* $u \cdot \epsilon \xrightarrow{1}{}^{*} u' \cdot \epsilon$ *alors pour tout contexte* C *de type approprié,* $u \cdot C \xrightarrow{1}{}^{*} u' \cdot C$.

Ceci nous permet de démontrer la proposition suivante.

Proposition 1 *Pour tout terme clos* u *de type* τ*, pour tout environnement* ρ*,* $u\ R_\tau\ [\![u]\!]\rho$.

Démonstration. Ceci s'effectue par récurrence sur le terme u. Nous ne traitons que de quelques cas. (La démontration réelle doit en fait établir un résultat plus général, et nécessite de plus une collection de lemmes auxiliaires que je préfère ne pas mentionner.) Si $u = \dot{n}$, avec $\tau = \mathtt{int}$, ceci est dû au fait que $\dot{n} \cdot \epsilon \xrightarrow{1}{}^{*} \dot{n} \cdot \epsilon$, qui est évident. Dans le cas d'une application uv, avec u de type $\sigma \to \tau$ et v de type τ, c'est par définition de $R_{\sigma\to\tau}$, en utilisant l'hypothèse de récurrence sur u et sur v. Dans le cas d'un terme $\dot{-}u$, avec u de type $\mathtt{int}$, on sait par hypothèse de récurrence que $u\ R_{\mathtt{int}}\ [\![u]\!]\rho$, c'est-à-dire que $[\![u]\!]\rho = \bot$, ou bien que $[\![u]\!]\rho$ est un entier n et que $u \cdot \epsilon \xrightarrow{1}{}^{*} \dot{n} \cdot \epsilon$. Dans ce dernier cas, par le lemme 5, $u \cdot \dot{-} \bullet \cdot \epsilon \xrightarrow{1}{}^{*} \dot{n} \cdot \dot{-} \bullet \cdot \epsilon$, et l'on ajoute devant cette trace l'instance $\dot{-}u \cdot \epsilon \xrightarrow{1} u \cdot \dot{-} \bullet \cdot \epsilon$ de la règle ($\dot{-}$?).

Question 15 [...]

[...]

Question 16 (***) Montrer que $\epsilon\ R^{\perp}_{\mathtt{int}}\ \eta_{[\![\mathtt{int}]\!]}$. Citer la ou les règles de sémantique opérationnelle utilisées.

Soit $v\ R_{\mathtt{int}}\ b$ *et* $n \in \mathbb{Z}$*. On doit démontrer que* $\Pr[\mathtt{ret}_{\mathtt{int}}\, v \cdot \epsilon \downarrow n] \geq \eta_{[\![\mathtt{int}]\!]}(b)(\mathbf{1}_n)$*. Si* $b \neq n$*, c'est évident : le côté droit vaut* 0*. Si* $b = n$*, le côté droit vaut* 1*, mais le côté gauche aussi : on a* $\mathtt{ret}_{\mathtt{int}}\, v \cdot \epsilon \xrightarrow{1} v \cdot \mathtt{ret}_{\mathtt{int}} \bullet$ *par la règle* (ret)*. Comme* $v\ R_{\mathtt{int}}\ b = n \neq \bot$*, on a* $v \cdot \epsilon \xrightarrow{1}{}^{*} \dot{n} \cdot \epsilon$*. Par le lemme 5, on en déduit* $v \cdot \mathtt{ret}_{\mathtt{int}} \bullet \xrightarrow{1}{}^{*} \dot{n} \cdot \mathtt{ret}_{\mathtt{int}} \bullet$*. On concatène ceci à* $\mathtt{ret}_{\mathtt{int}}\, v \cdot \epsilon \xrightarrow{1} v \cdot \mathtt{ret}_{\mathtt{int}} \bullet$*, et l'on obtient* $\mathtt{ret}_{\mathtt{int}}\, v \cdot \epsilon \xrightarrow{1}{}^{*} \dot{n} \cdot \mathtt{ret}_{\mathtt{int}} \bullet$*. Donc* $\Pr[\mathtt{ret}_{\mathtt{int}}\, v \cdot \epsilon \downarrow^{\leq K} n]$ *vaut* 1 *pour tout* $K \geq 1$*, et en particulier* $\Pr[\mathtt{ret}_{\mathtt{int}}\, v \cdot \epsilon \downarrow n] \geq 1$.

Question 17 [...]

[redacted] *[...]*

[...] [...]

Question 18 [...]

[redacted] *[...]*