Examen Programmation I (2023-24)

Cet examen se déroule en deux parties. Ceci est la deuxième partie. Pas la peine de répondre aux questions de la première partie (en petit). 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.

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 $a + b \leq 1$.

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 $(*)$ Soient $a, b \in \underline{\mathbb{I}}$ tels que $a + b \leq 1$. On admettra que la fonction qui à $(s,t) \in \underline{\mathbb{I}} \times \underline{\mathbb{I}}$ associe $as + bt$ est Scott-continue. Montrer que pour toute famille dirigée $(F_i)_{i \in I}$ de distributions sur X, la fonction F définie par :

$$F(h) = \sup_{i \in I} F_i(h)$$

pour toute $h \in [X \to \underline{\mathbb{I}}]$, est une distribution.

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.*

Pour tout $x \in X$, on note δ_x la fonction qui à tout $h \in [X \to \underline{\mathbb{I}}]$ associe $h(x)$. C'est la *distribution de Dirac en x*.

Question 2 $(*)$ On définit $\eta_X \colon X \to \mathbf{D}(X)$ par $\eta_X(x) \stackrel{\text{def}}{=} \delta_x$ pour tout $x \in X$. Montrer que η_X est Scott-continue.

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 $\mathbf{D}(Y)$.*

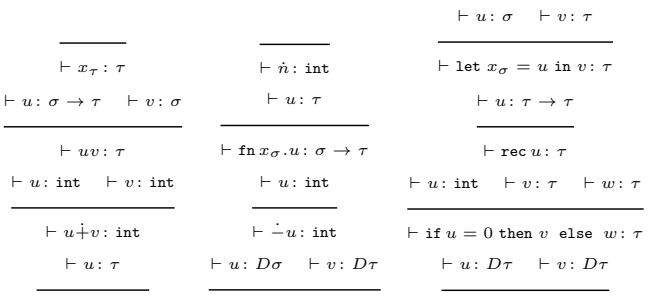

FIGURE 1 – Les expressions de PCF+distributions avec leurs types

Question 3 (∗) Montrer que, pour tous dcpos X et Y, pour toute fonction $f \in [X \to \mathbf{D}(Y)]$, $f^\dagger$ est elle-même *linéaire*, au sens pour toutes distributions $F, G \in \mathbf{D}(X)$, pour tous $a, b \in \mathbb{I}$ tels que $a + b \leq 1$,

$$f^\dagger(aF + bG) = af^\dagger(F) + bf^\dagger(G).$$

On note $aF + bG$ la distribution $h \in [X \to \mathbb{I}] \mapsto aF(h) + bG(h)$.

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 $[[X \to \mathbb{I}], k$ de $[Y \to \mathbb{I}], \ell$ de $[Z \to \mathbb{I}]$, x de X, y de Y, z de Z.

On admettra que les égalités suivantes sont elles aussi valides :

$$\eta^\dagger_X = \mathrm{id}_{\mathbf{D}X} \tag{4}$$

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

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

Les types sont :

$\sigma, \tau, \cdots ::= \mathtt{int}$	entiers
$\mid \sigma \to \tau$	functions
$\mid D\tau$	distributions (nouveau).

La sémantique dénotationnelle des types est donnée par :

- $[\![\mathtt{int}]\!] = \mathbb{Z}_\perp$; $\mathbb{Z}$ 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 (∗) Montrer que $[\![\tau]\!]$ est un dcpo, pour tout type τ.

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 $h \in [X \to \mathbb{I}] \mapsto \frac{1}{2}F(h) + \frac{1}{2}G(h)$.

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

$$uv \cdot C \xrightarrow{1} u \cdot \bullet\, v \cdot C \quad (app?) \qquad (\texttt{fn}\, x_\sigma.u) \cdot \bullet\, v \cdot C \xrightarrow{1} u[x_\sigma := v] \cdot C \quad (app!)$$
$$\texttt{let}\ x_\sigma = u\ \texttt{in}\ v \cdot C \xrightarrow{1} v[x_\sigma := u] \cdot C \quad (\texttt{let})$$
$$\texttt{rec}\, u \cdot C \xrightarrow{1} u(\texttt{rec}\, u) \cdot C \quad (\texttt{rec})$$
$$\dot{-} u \cdot C \xrightarrow{1} u \cdot \dot{-}\bullet \cdot C \quad (\dot{-}?) \qquad \dot{n} \cdot \dot{-}\bullet \cdot C \xrightarrow{1} \overbrace{-n} \cdot C \quad (\dot{-}!)$$
$$u \dot{+} v \cdot C \xrightarrow{1} u \cdot \bullet \dot{+} v \cdot C \quad (\dot{+}?_1) \qquad \dot{m} \cdot \bullet \dot{+} v \cdot C \xrightarrow{1} v \cdot \dot{m} \dot{+} \bullet \cdot C \quad (\dot{+}?_2)$$
$$\dot{n} \cdot \dot{m} \dot{+} \bullet \cdot C \xrightarrow{1} \overbrace{m + n} \cdot C$$
$$\texttt{if}\ u = 0\ \texttt{then}\ v\ \texttt{else}\ w \cdot C \xrightarrow{1} u \cdot \texttt{if} \bullet = 0\ \texttt{then}\ v\ \texttt{else}\ w \cdot C \quad (\texttt{if}?)$$
$$\dot{0} \cdot \texttt{if} \bullet = 0\ \texttt{then}\ v\ \texttt{else}\ w \cdot C \xrightarrow{1} v \cdot C \quad (\texttt{if}!_{=0})$$
$$\dot{n} \cdot \texttt{if} \bullet = 0\ \texttt{then}\ v\ \texttt{else}\ w \cdot C \xrightarrow{1} w \cdot C \quad \text{si } n \neq 0 \quad (\texttt{if}!_{\neq 0})$$
$$\texttt{do}\, x_\sigma \leftarrow u; v \cdot C \xrightarrow{1} u \cdot \texttt{do}\, x_\sigma \leftarrow \bullet; v \cdot C \quad (\texttt{do}?)$$
$$\texttt{ret}_\sigma\, u \cdot \texttt{do}\, x_\sigma \leftarrow \bullet; v \cdot C \xrightarrow{1} v[x_\sigma := u] \cdot C \quad (\texttt{do}!)$$
$$u \oplus v \cdot C \xrightarrow{1/2} u \cdot C \quad (\oplus_1) \qquad u \oplus v \cdot C \xrightarrow{1/2} v \cdot C \quad (\oplus_2)$$
$$\texttt{ret}_\tau\, u \cdot \epsilon \xrightarrow{1} u \cdot \texttt{ret}_\tau \bullet \quad (\texttt{ret})$$

FIGURE 3 – Sémantique opérationnelle

Question 6 (∗) Pourquoi le plus petit point fixe $\mathrm{lfp}(\llbracket u \rrbracket\rho)$ existe-t-il dans la définition de $\llbracket \texttt{rec}\, u \rrbracket\rho$? On donnera le nom du théorème utilisé, et on vérifiera ses hypothèses.

Question 7 (∗) 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 $F \in \mathbf{D}(\mathbb{Z}_\perp) \mapsto (h \in [\mathbb{Z}_\perp \to \mathbb{I}] \mapsto \frac{1}{4}(h(1) + h(2) + h(3) + F(h))$?

(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.

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

$$\frac{}{\vdash \epsilon : \lambda \Rightarrow \lambda} \qquad \frac{}{\vdash \texttt{ret}_\tau \bullet : \tau \Rightarrow D\tau}$$
$$\frac{\vdash C : D\tau \Rightarrow \lambda}{\vdash \texttt{do}\, x_\sigma \leftarrow \bullet; v \cdot C : D\sigma \Rightarrow \lambda} \qquad \frac{\vdash C : \tau \Rightarrow \lambda \quad \vdash v : \sigma}{\vdash \bullet\, v : (\sigma \to \tau) \cdot C \Rightarrow \lambda} \qquad \frac{\vdash C : \texttt{int} \Rightarrow \lambda}{\vdash \dot{-}\bullet \cdot C : \texttt{int} \Rightarrow \lambda}$$
$$\frac{\vdash C : \texttt{int} \Rightarrow \lambda \quad \vdash v : \texttt{int}}{\vdash \bullet \dot{+} v \cdot C : \texttt{int} \Rightarrow \lambda} \qquad \frac{\vdash C : \texttt{int} \Rightarrow \lambda}{\vdash \dot{m} \dot{+} \bullet \cdot C : \texttt{int} \Rightarrow \lambda} \qquad \frac{\vdash C : \tau \Rightarrow \lambda \quad \vdash v : \tau \quad \vdash w : \tau}{\vdash \texttt{if} \bullet = 0\ \texttt{then}\ v\ \texttt{else}\ w \cdot C : \texttt{int} \Rightarrow \lambda}$$

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 8 $(*)$ Montrer que la règle $(\mathtt{rec})$ est *correcte*, autrement dit que $[\![\mathtt{rec}\, u \cdot C]\!]\rho = [\![u \cdot \bullet\, (\mathtt{rec}\, u) \cdot C]\!]\rho$ (quels que soient u, C, ρ tels que ces objets aient un sens).

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*,* $[\![s]\!]\rho = [\![t]\!]\rho$*.*

Pour ce qui est des autres règles, c'est-à-dire $(\oplus_1)$ et $(\oplus_2)$, elles sont traitées aux questions suivantes.

Question 9 $(**)$ Quelle est la forme générale des contextes C de type $D\tau \Rightarrow D\mathtt{int}$? Le type τ est arbitraire. La solution à cette question de la première partie était :

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

où ϵ est de type $D\mathtt{int} \Rightarrow D\mathtt{int}$, où les termes $v_1, \ldots, v_n$ sont de types appropriés.

Question 10 $(**)$ Montrer que tous les contextes C de type $D\tau \Rightarrow D\mathtt{int}$ sont linéaires, autrement dit $[\![C]\!]\rho(aF + bG) = a[\![C]\!](\rho)(F) + b[\![C]\!]\rho(G)$ pour tous environnements ρ, toutes distributions $F, G \in \mathbf{D}([\![\tau]\!])$, et tous $a, b \in \mathbb{I}$ tels que $a + b \leq 1$.

Question 11 (∗) Montrer pour tous termes $u, v\colon D\tau$, pour tout contexte $C\colon D\tau \Rightarrow D\mathtt{int}$, pour tout environnement ρ,

$$[\![u \oplus v \cdot C]\!]\rho = \frac{1}{2}[\![u \cdot C]\!]\rho + \frac{1}{2}[\![v \cdot C]\!]\rho.$$

Question 12 (∗∗∗) Montrer que, pour toute configuration s de type $D\mathtt{int}$, pour tout $n \in \mathbb{N}$, pour tout environnement ρ, $\Pr[s \downarrow n] \leq [\![s]\!]\rho(\mathbf{1}_n)$, où $\mathbf{1}_n \in [\mathtt{int} \to \underline{\mathbb{I}}]$ est la fonction qui à n associe 1, et à tout autre élément de $\mathbb{Z}_\perp$ associe 0. (On admettra que $\mathbf{1}_n$ est Scott-continue.)

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 $\ll$ pour touts $a\ R_\tau\ b \gg$ pour dire $\ll$ pour tous a et b [dans les ensembles appropriés] tels que $a\ R_\tau\ b \gg$.

- $u\ R_{\mathtt{int}}\ n$ 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 13 (∗∗) Terminer la démonstration du lemme 4 et traiter du cas des types de la forme $D\tau$.

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 $[\![u]\!]\rho = \perp$, 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 ($\dot{-}$?).

$$\frac{}{\Gamma, x\colon \tau \vdash x\colon \tau} \qquad \frac{}{\Gamma \vdash \dot{n}\colon \texttt{int}} \qquad \frac{\Gamma \vdash u\colon \sigma \quad \Gamma \vdash v\colon \tau}{\Gamma \vdash \texttt{let}\ x = u\ \texttt{in}\ v\colon \tau}$$

$$\frac{\Gamma \vdash u\colon \sigma \to \tau \quad \Gamma \vdash v\colon \sigma}{\Gamma \vdash uv\colon \tau} \qquad \frac{\Gamma, x\colon \sigma \vdash u\colon \tau}{\Gamma \vdash \texttt{fn}\, x.u\colon \sigma \to \tau} \qquad \frac{\Gamma \vdash u\colon \tau \to \tau}{\Gamma \vdash \texttt{rec}\, u\colon \tau}$$

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

$$\frac{\Gamma \vdash u\colon \tau}{\Gamma \vdash \texttt{ret}\, u\colon D\tau} \qquad \frac{\Gamma \vdash u\colon D\sigma \quad \Gamma \vdash v\colon D\tau}{\Gamma, x\colon \sigma \vdash \texttt{do}\, x \leftarrow u; v\ \colon D\tau} \qquad \frac{\Gamma \vdash u\colon D\tau \quad \Gamma \vdash v\colon D\tau}{\Gamma \vdash u \oplus v\colon D\tau}$$

FIGURE 4 – Les expressions de pureML+distributions avec leurs types

Question 14 (∗∗∗) Écrire le cas de la démonstration de la proposition 1 concernant la récursion. Autrement dit, sachant que $u\ R_{\tau\to\tau}\ [\![u]\!]\rho$ (par hypothèse de récurrence), montrer que $\texttt{rec}\, u\ R_\tau\ [\![\texttt{rec}\, u]\!]\rho$. On nommera explicitement la ou les règles de sémantique opérationnelle utilisées. On pourra utiliser sans avoir à le démontrer le lemme suivant : (A) si $v\cdot\epsilon \xrightarrow{1}{}^{*} w\cdot\epsilon$ et $w\ R_\tau\ a$ alors $v\ R_\tau\ a$.

Question 15 (∗∗∗) Montrer que $\epsilon\ R^{\perp}_{\texttt{int}}\ \eta_{[\![\texttt{int}]\!]}$. Citer la ou les règles de sémantique opérationnelle utilisées.

Question 16 (∗∗) En déduire le théorème de correction et d'adéquation : pour tout terme clos u de type $D\texttt{int}$, pour tout environnement ρ, pour tout $n \in \mathbb{N}$, $\Pr[u \cdot \epsilon \downarrow n] = [\![u]\!]\rho(\mathbf{1}_n)$. Comme d'habitude, citez les résultats utilisés.

On termine par une question portant sur le typage. On considère le langage pureML+distributions, obtenu en enlevant les indices de typage des termes PCF+distributions. Les règles de typage sont celles de la figure 4.

Question 17 (∗∗) Décrire un algorithme en temps polynomial permettant de décider, étant donner un terme u_0 de pureML+distributions, s'il est typable, et si oui d'en donner un typage principal. J'attends un algorithme similaire à un algorithme vu en cours ; dans ce cas, il est inutile d'en donner la preuve.