

# Examen Programmation I (2020-21)

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. Pour tout raisonnement par récurrence, on devra dire sur quoi est effectuée la récurrence. 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, pas de questions dans le désordre, notamment. Je corrigerai très probablement 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 souviens de ce que vous avez écrit dans une question précédente.

Je me réserve le droit de ne pas chercher à comprendre une réponse illisible, insuffisamment claire, ou plus longue ou compliquée que nécessaire.

J'appellerai *fonction* ce qu'on appelle plus communément une application, c'est-à-dire une fonction totale.

## 1 Prolog

On considère le langage suivant, qui est un sous-ensemble de Prolog. On rappelle la notion de terme, vue en cours dans le cadre du système de typage de ML. L'ensemble  $\mathcal{T}(\Sigma, X)$  des termes  $s, t, u, v, \dots$  est défini inductivement par : les variables  $x, y, z, \dots$  de  $X$  sont des termes de  $\mathcal{T}(\Sigma, X)$ , et les *applications*  $f(t_1, \dots, t_n)$  de  $f$  (avec  $f/n$  dans la signature  $\Sigma$ ) à  $n$  termes  $t_1, \dots, t_n$  de  $\mathcal{T}(\Sigma, X)$  sont dans  $\mathcal{T}(\Sigma, X)$ .

On supposera dans la suite que  $\Sigma$  contient au moins une constante  $a/0$ . L'ensemble  $\mathcal{T}(\Sigma)$  des *termes clos*, défini comme égal à  $\mathcal{T}(\Sigma, \emptyset)$ , est alors non vide.

Un *atome*  $A$  est juste une application  $p(t_1, \dots, t_n)$ , et  $p$  s'appelle le *prédicat* de l'atome. On notera  $\Pi$  l'ensemble des prédicats. Une *clause définie* est une expression de la forme  $A :- A_1, \dots, A_m$ . où  $A, A_1, \dots, A_m$  sont des atomes. (L'entier  $m$  peut être nul, auquel cas on écrira juste  $A$  : ce genre de clause définie s'appelle un *fait*.) L'atome  $A$  forme la *tête* de cette clause définie, et  $A_1, \dots, A_m$  est son *corps*.

Un *programme Prolog* est juste une liste finie de clauses définies. On peut lire un programme Prolog de deux façons : soit comme une axiomatisation logique, où une clause définie comme ci-dessus se lira «  $A_1$  et  $\dots$  et  $A_m$  impliquent logiquement  $A$  » ; soit comme un programme exécutable.

Par exemple, le programme Prolog suivant :

```
append(nil,L,L).
append(cons(X,L),L',cons(X,L')) :- append(L,L',L').
```

définit logiquement `append` de sorte que `append( $\ell_1, \ell_2, \ell_3$ )` soit vrai si et seulement si  $\ell_3$  est la concaténation des listes  $\ell_1$  et  $\ell_2$ . (Par convention les fonctions de  $\Sigma$  sont les noms commençant par une minuscule, et les variables commencent par une majuscule.) On peut l'utiliser pour *calculer* la concaténation de listes : si l'on entre le programme Prolog ci-dessus dans, par exemple, SWI-Prolog, et que l'on tape :

```
? append(cons(1,nil), cons(2,cons(3,nil)), Resultat).
```

SWI-Prolog va répondre :

```
yes
Resultat = cons(1,cons(2,cons(3,nil)))
```

Dans cette partie, on se fixe un programme Prolog  $P$ .

On appellera *environnement*  $\rho$  toute fonction des variables vers les termes clos. On définit l'application  $t\rho$  d'un environnement  $\rho$  à un terme  $t$  exactement comme pour les substitutions. En général, on manipulera les environnements exactement comme les substitutions.

On notera que  $t\rho$  est toujours un terme clos. On étendra la notion d'application de substitutions et d'environnements à tout atome, toute clause, de la façon évidente.

Pour tout  $E \in \mathbb{P}(\mathcal{T}(\Sigma))$ , définissons un ensemble  $T_P(E)$  comme suit. Voici d'abord l'idée intuitive.  $E$  est typiquement l'ensemble des atomes clos dont on sait qu'ils sont vrais, parce qu'ils ont été déduits en, disons,  $k$  étapes à partir des faits de  $P$ .  $T_P(E)$  est l'ensemble des atomes clos déduits de ceux de  $E$  à l'aide d'une clause définie de  $P$ , en une étape ; si  $E$  est comme ci-dessus,  $T_P(E)$  sera donc l'ensemble des atomes clos déduits en  $k+1$  étapes à partir des faits de  $P$ . Formellement (et seule cette définition compte pour le raisonnement !) :

$$T_P(E) = \{A\rho \mid \rho \text{ environnement, et il existe une clause définie } (A :- A_1, \dots, A_n) \in P \text{ de tête } A \text{ et telle que } A_1\rho, \dots, A_n\rho \in E\}.$$

On munit  $\mathbb{P}(\mathcal{T}(\Sigma))$  de l'ordre  $\subseteq$ , ce qui en fait un treillis complet, et donc un dcpo.

**Question 1** Montrer que  $T_P$  est Scott-continue.

**Question 2** Pourquoi le plus petit point fixe de  $T_P$  existe-t-il ?

On notera  $\text{lfp}(T_P)$  le plus petit point fixe de  $T_P$ . C'est, intuitivement, l'ensemble des atomes clos *vrais* dans l'interprétation logique de  $P$ . C'est aussi, de façon plus banale, la sémantique dénotationnelle du programme Prolog  $P$ .

Etant donné un *but*, c'est-à-dire un atome  $B$ , pas nécessairement clos, précédé du symbole ? (comme ? `append(cons(1,nil), cons(2,cons(3,nil)), Resultat)`, avec une variable `Resultat`), Prolog va chercher des valeurs des variables dans  $B$  rendant  $B$  vrai. Formellement, Prolog va chercher s'il existe un environnement  $\rho$  tel que  $B\rho \in \text{lfp}(T_P)$  (et en retourner un, restreint aux variables de  $B$ , s'il en existe un).

On note  $\text{mgu}(A \doteq B)$  l'unificateur le plus général (le mgu) de l'équation  $A \doteq B$ . On a vu la notion en cours pour des équations entre termes. Ici il s'agit d'équations entre atomes : l'extension aux atomes est triviale.

**Question 3** Supposons qu'aucune variable n'apparaisse à la fois dans l'atome  $B$  et dans le programme  $P$ . On notera aussi  $\text{vars}(B)$  l'ensemble des variables apparaissant dans  $B$ , et de même  $\text{vars}(P)$ , etc.

Montrer que si  $B\rho \in \text{lfp}(T_P)$ , alors : (i) il existe une clause définie  $A :- A_1, A_2, \dots, A_n$  dans  $P$  telle que l'équation  $B \doteq A$  soit unifiable ; (ii) en posant  $\theta = \text{mgu}(B \doteq A)$ ,  $B\rho$  s'écrit  $B\theta\rho'$  pour un certain environnement  $\rho'$  ; (iii)  $A_1\theta\rho', \dots, A_n\theta\rho'$  sont tous dans  $\text{lfp}(T_P)$ .

Pour une clause définie  $C$  de  $P$  et un atome  $B$ , on appellera *renommage de  $C$  loin de  $B$*  une clause de la forme  $C\rho$ , où  $\rho$  est un renommage (une substitution qui envoie les variables vers des variables, et qui est injective sur l'ensemble des variables libres de  $C$ ), de sorte qu'il n'y ait aucune variable en commun entre  $C\rho$  et  $B$ .

On définit une sémantique opérationnelle de Prolog comme suit. Une configuration  $C$  de cette sémantique est un multi-ensemble fini de buts. L'unique règle, dite de *résolution*, est :

$$C \cup \{?B\} \xrightarrow{\theta} C\theta \cup \{?A_1\theta, \dots, ?A_n\theta\}$$

où  $A :- A_1, A_2, \dots, A_n$  est un renommage d'une clause définie dans  $P$  loin de  $B$ , et  $\theta = \text{mgu}(B \doteq A)$ . (Oui, la sémantique est non déterministe : on ne précise pas comment choisir le but  $?B$  dans la configuration.) Noter qu'on a pris soin d'étiqueter la transition par le mgu  $\theta$  : ce sera parfois pratique dans la suite. On notera  $C \rightarrow C'$  pour dire que  $C \xrightarrow{\theta} C'$  pour une certaine substitution  $\theta$ , si elle n'est pas importante. Ceci permet de définir la clôture réflexive-transitive  $\rightarrow^*$ , notamment.

On appellera *instance* d'un but  $?A$  tout atome clos de la forme  $A\rho$ , où  $\rho$  est un environnement. On appellera  $A\rho$  plus précisément une  $\rho$ -instance de  $A$  lorsqu'on veut mentionner  $\rho$  explicitement.

**Question 4** Montrer que la règle de résolution est correcte, au sens où, pour tout environnement  $\rho$ , si toutes les  $\rho$ -instances du côté droit  $C\theta \cup \{?A_1\theta, \dots, ?A_n\theta\}$  sont dans  $\text{lfp}(T_P)$ , alors toutes les  $\theta\rho$ -instances du côté gauche  $C \cup \{?B\}$  sont aussi dans  $\text{lfp}(T_P)$ .

**Question 5** En déduire que la sémantique opérationnelle de Prolog est correcte : si  $\{?B\} \rightarrow^* \emptyset$ , et plus précisément si  $\{?B\} = C_0 \xrightarrow{\theta_1} C_1 \xrightarrow{\theta_2} \dots \xrightarrow{\theta_m} C_m = \emptyset$ , alors il existe une substitution  $\theta$  telle que, pour tout environnement  $\rho$ ,  $B\theta\rho$  est dans  $\text{lfp}(T_P)$ . On construira  $\theta$  explicitement.

Dans ce cas, Prolog répond **yes** suivi de la restriction de  $\theta$  à  $\text{vars}(B)$ .

**Question 6** En adaptant la **Question 3**, montrer que la sémantique opérationnelle de Prolog est aussi adéquate : si  $B\rho$  est une instance de  $?B$  dans  $\text{lfp}(T_P)$ , alors  $\{?B\} \rightarrow^* \emptyset$ . On montrera plus précisément que si  $B\rho$  est une instance de  $?B$  dans  $\text{lfp}(T_P)$ , alors il existe un nombre fini d'étapes  $\{?B\} = C_0 \xrightarrow{\theta_1} C_1 \xrightarrow{\theta_2} \dots \xrightarrow{\theta_m} C_m = \emptyset$  et un environnement  $\rho'$  tel que  $\rho = \theta_1\theta_2 \dots \theta_m\rho'$ .

## 2 Boules formelles

Le but de cette section est de montrer que les dcpos interviennent naturellement en mathématiques, pas seulement en informatique. Soit  $X$  un espace métrique, dont la distance sera notée  $d$ . Autrement dit,  $d$  est une fonction de  $X^2$  dans  $\mathbb{R}_+$  telle que, pour tous  $x, y, z \in X$  :

- $d(x, y) = 0$  si et seulement si  $x = y$  ;
- $d(x, y) = d(y, x)$  ;

—  $d(x, z) \leq d(x, y) + d(y, z)$  (inégalité triangulaire).

Il se trouve que les notions suivantes ne sont plus au programme des classes préparatoires, définissons-les donc. Soit  $(x_n)_{n \in \mathbb{N}}$  une suite de points dans  $X$ . On dit qu'un point  $x_\infty$  de  $X$  est une *limite* de cette suite si et seulement si pour tout  $\epsilon > 0$ , il existe un  $n_0 \in \mathbb{N}$  tel que pour tout  $n \geq n_0$ ,  $d(x_n, x_\infty) \leq \epsilon$ . (On dira, pour abrégé : « pour tout  $\epsilon > 0$ , pour tout  $n$  assez grand,  $d(x_n, x_\infty) \leq \epsilon$  ».) La limite, si elle existe, est alors unique, et on dit aussi que la suite *converge* vers sa limite ou *est convergente*. La suite est *de Cauchy* si et seulement si pour tout  $\epsilon > 0$ , il existe un  $n_0 \in \mathbb{N}$  tel que pour tous  $i, j \geq n_0$ ,  $d(x_i, x_j) \leq \epsilon$ . Toute suite convergente est de Cauchy. Un espace dans lequel toute suite de Cauchy est convergente et appelé un espace métrique *complet*.  $\mathbb{R}$ , muni de sa distance usuelle, est un espace métrique complet ;  $\mathbb{Q}$ , en revanche, non.

Passons à notre sujet. Au lieu de vous faire démontrer la totalité des résultats, je vous demanderai d'en démontrer une partie, et je vous donnerai une idée des arguments manquants.

Une *boule formelle* est un couple  $(x, r)$  où  $x \in X$  et  $r \in \mathbb{R}_+$ . On peut imaginer qu'il s'agisse de la spécification de la boule fermée de centre  $x$  et de rayon  $r$ , mais l'analogie, quoiqu'utile, aura ses limites.

On pose  $\mathbf{B}(X)$  l'ensemble de toutes les boules formelles, et on définit la relation  $\sqsubseteq$  par  $(x, r) \sqsubseteq (y, s)$  si et seulement si  $d(x, y) \leq r - s$ . (On notera au passage que ceci implique  $r \geq s$ .) Il s'agit toujours d'une relation d'ordre. Cela ne saute pas forcément aux yeux, et je vous incite à vous familiariser avec cette notion en démontrant que  $\sqsubseteq$  est transitive d'abord, antisymétrique ensuite.

**Question 7** Soit  $D$  une famille dirigée de boules formelles. On pose  $r_\infty \stackrel{\text{def}}{=} \inf\{r \mid (x, r) \in D\}$ . Justifier les affirmations suivantes :

- (a) Pour tout  $n \in \mathbb{N}$ , il existe une boule formelle  $(x'_n, r'_n)$  dans  $D$  telle que  $r'_n \leq r_\infty + 1/2^n$ .
- (b) On peut trouver une suite *croissante* d'éléments  $(x_n, r_n)$  de  $D$  tels que  $r_n \leq r_\infty + 1/2^n$  pour tout  $n \in \mathbb{N}$ .
- (c) Les majorants  $(y, s)$  de  $D$  sont exactement les majorants de la suite  $\{(x_n, r_n) \mid n \in \mathbb{N}\}$ .

On aura besoin du fait suivant, que vous n'aurez pas à démontrer. Vous pouvez, et devez, le citer explicitement à tout moment où il vous sera utile. De même pour les autres faits qui seront énoncés plus loin.

**Fait 1** Soit  $X$  un espace métrique, de distance  $d$ . Pour toute suite croissante  $(x_n, r_n)$ ,  $n \in \mathbb{N}$ , dans  $\mathbf{B}(X)$ ,  $(x_n)_{n \in \mathbb{N}}$  est une suite de Cauchy dans  $X$ .

*Démonstration.* Soit  $r_\infty \stackrel{\text{def}}{=} \inf_{n \in \mathbb{N}} r_n$ . La suite  $(r_n)_{n \in \mathbb{N}}$  est décroissante. Fixons  $\epsilon > 0$ . On a alors  $r_n \leq r_\infty + \epsilon$  pour  $n$  assez grand, disons  $n \geq n_0$ . Pour tous  $i, j \geq n_0$ , disons  $i \leq j$  par symétrie, on a donc  $(x_i, r_i) \sqsubseteq (x_j, r_j)$  donc  $d(x_i, x_j) \leq r_i - r_j \leq r_i - r_\infty \leq \epsilon$ .  $\square$

**Question 8** Montrer que pour toute suite croissante  $(x_n, r_n)$ ,  $n \in \mathbb{N}$ , dans  $\mathbf{B}(X)$ , si  $(x_n)_{n \in \mathbb{N}}$  converge vers un point  $x_\infty$  de  $X$ , alors  $(x_\infty, r_\infty)$  est la borne supérieure de la famille  $(x_n, r_n)_{n \in \mathbb{N}}$  dans  $\mathbf{B}(X)$ , où  $r_\infty \stackrel{\text{def}}{=} \inf_{n \in \mathbb{N}} r_n$ .

Voici deux nouveaux faits utiles, dont je vous donne aussi les démonstrations.

**Fait 2** Soit  $X$  un espace métrique, de distance  $d$ . De toute suite de Cauchy  $(x_n)_{n \in \mathbb{N}}$  dans  $X$  on peut extraire une sous-suite  $(x_{n_k})_{k \in \mathbb{N}}$  (i.e.,  $n_0 < n_1 < \dots < n_k < \dots$ ) telle que  $(x_{n_k}, 1/2^k)_{k \in \mathbb{N}}$  soit une famille dirigée, et en fait une suite croissante, dans  $\mathbf{B}(X)$ .

*Démonstration.* On construit  $n_k$  par récurrence sur  $k$ . Comme  $(x_n)_{n \in \mathbb{N}}$  est de Cauchy, il existe un entier  $n_0$  tel que pour tous  $i, j \geq n_0$ ,  $d(x_i, x_j) \leq 1/2^1$ .

Il existe ensuite un entier  $n_1$  tel que pour tous  $i, j \geq n_1$ ,  $d(x_i, x_j) \leq 1/2^2$ , et on peut choisir  $n_1 > n_0$ .

De proche en proche (c'est-à-dire, formellement, par une récurrence sur  $k$ ), on trouve  $n_k > n_{k-1}, \dots, n_0$  tel que pour tous  $i, j \geq n_k$ ,  $d(x_i, x_j) \leq 1/2^{k+1}$ .

En particulier, pour tout  $k \geq 1$ ,  $d(x_{n_{k-1}}, x_{n_k}) \leq 1/2^k$ . Or  $1/2^k = 1/2^{k-1} - 1/2^k$ , donc  $(x_{n_{k-1}}, 1/2^{k-1}) \sqsubseteq (x_{n_k}, 1/2^k)$ .  $\square$ .

**Fait 3** Soit  $X$  un espace métrique, de distance  $d$ . Pour toute suite de Cauchy  $(x_n)_{n \in \mathbb{N}}$  dans  $X$ , s'il en existe une sous-suite  $(x_{n_k})_{k \in \mathbb{N}}$  qui converge vers une limite  $x_\infty$ , alors  $(x_n)_{n \in \mathbb{N}}$  elle-même converge vers  $x_\infty$ .

*Démonstration.* Pour tout  $\epsilon > 0$ , en utilisant que  $(x_n)_{n \in \mathbb{N}}$  est de Cauchy, on a  $d(x_n, x_m) \leq \epsilon/2$  pour tous  $n, m$  assez grands, disons plus grands que  $n_0$ . Comme  $(x_{n_k})_{k \in \mathbb{N}}$  converge vers  $x_\infty$ , on a aussi  $d(x_{n_k}, x_\infty) \leq \epsilon/2$  pour  $k$  assez grand, disons plus grand que  $k_0$ . On choisit un tel  $k$  plus grand que  $k_0$  de sorte que  $n_k$  soit plus grand que  $n_0$ . En posant  $m \stackrel{\text{def}}{=} n_k$ , pour tout  $n$  plus grand que  $n_0$ , on a alors  $d(x_n, x_\infty) \leq d(x_n, x_{n_k}) + d(x_{n_k}, x_\infty) \leq \epsilon/2 + \epsilon/2 = \epsilon$ .  $\square$

**Question 9** Montrer que si  $(x_n, r_n)_{n \in \mathbb{N}}$  est une suite croissante dans  $\mathbf{B}(X)$  et si  $\inf_{n \in \mathbb{N}} r_n = 0$ , alors la famille  $(x_n, r_n)_{n \in \mathbb{N}}$  a au plus un majorant ; que s'il existe, il est de la forme  $(x_\infty, 0)$ , et que  $x_\infty$  est alors une (la) limite de  $(x_n)_{n \in \mathbb{N}}$  dans  $X$ .

**Question 10** En déduire que  $\mathbf{B}(X)$  est un dcpo si et seulement si  $X$  est un espace métrique complet.

De cela, on peut déduire des théorèmes de point fixe intéressants. Par exemple, si  $X$  est un espace métrique complet et  $f$  est une fonction  $\alpha$ -lipschitzienne de  $X$  dans  $X$  (i.e.,  $d(f(x), f(y)) \leq \alpha \cdot d(x, y)$  pour tous  $x, y \in X$ ) avec  $0 \leq \alpha < 1$ , on peut vérifier que la fonction  $\mathbf{B}_\alpha f: \mathbf{B}(X) \rightarrow \mathbf{B}(X)$  qui à  $(x, r)$  associe  $(f(x), \alpha r)$  est Scott-continue. Si  $x$  est n'importe quel point de  $X$ , en posant  $r \stackrel{\text{def}}{=} d(x, f(x))/(1 - \alpha)$ , on peut vérifier que la suite des points  $(\mathbf{B}_\alpha f)^n(x, r)$ ,  $n \in \mathbb{N}$ , est croissante dans  $\mathbf{B}(X)$ . Par la **Question 10**, elle aura une borne supérieure, qui est nécessairement un point fixe de  $\mathbf{B}_\alpha f$ . Or les seuls points fixes de  $\mathbf{B}_\alpha f$  sont les boules formelles de la forme  $(x, 0)$  où  $x$  est un point fixe de  $f$ . On retrouve ainsi le théorème du point fixe de Banach... par une démonstration bien plus compliquée que la démonstration usuelle.

Voici un théorème beaucoup plus fin. On aura besoin du *théorème de Bourbaki-Witt*, que certains d'entre vous ont vu en cours de mathématiques discrètes. Il énonce que, pour tout ensemble ordonné inductif  $P$  (par exemple, un dcpo), pour toute fonction  $f: P \rightarrow P$  inflationnaire (c'est-à-dire telle que  $p \leq f(p)$  pour tout  $p \in P$ ;  $f$  n'est pas nécessairement croissante), pour tout  $p_0 \in P$ ,  $f$  a un point fixe  $p$  tel que  $p_0 \leq p$ .

Un *potentiel* sur  $X$  est une fonction  $\pi: X \rightarrow \mathbb{R}_+$  semi-continue inférieurement, c'est-à-dire telle que pour toute suite  $(x_n)_{n \in \mathbb{N}}$  qui a une limite  $x_\infty$  dans  $X$ , pour tout  $\epsilon > 0$ , on a  $\pi(x_n) \geq \pi(x_\infty) - \epsilon$  pour tout  $n$  assez grand.

**Question 11** Soit  $X$  un espace métrique complet non vide,  $f: X \rightarrow X$  une fonction quelconque (pas nécessairement lipschitzienne, continue, ou rien) de  $X$  dans  $X$ , et  $\pi$  un potentiel tel que

pour tout  $x \in X$ ,  $d(x, f(x)) \leq \pi(x) - \pi(f(x))$ . Montrer qu'alors  $f$  a un point fixe. C'est le *théorème de Caristi*. À titre d'indication, montrer que  $Z \stackrel{\text{def}}{=} \{(x, r) \in \mathbf{B}(X) \mid r \geq \pi(x)\}$  est un dcpo dans l'ordre  $\sqsubseteq$ . Si vous ne voyez pas à quoi ça sert, vous avez peut-être raté un point subtil de la démonstration. Vous devriez être capable de montrer que pour tout point  $x_0$  de  $X$ , il existe même un tel point fixe de  $f$  à distance au plus  $\pi(x_0)$  de  $x_0$ .